(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 July 2001 (05.07.2001)

PCT

(10) International Publication Number
WO 01/48628 A2

(51) International Patent Classification⁷: G06F 17/00

(21) International Application Number: PCT/US00/28954

(22) International Filing Date: 19 October 2000 (19.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/471,744	23 December 1999 (23.12.1999)	US
PCT/US00/10678	19 April 2000 (19.04.2000)	US
09/614,302	12 July 2000 (12.07.2000)	US

(71) Applicant: BARTON, Peter, R. [US/US]; 1 Pond Road, Englewood, CO 80110 (US).

(74) Agents: AMES, Wesley, B. et al.; Brobeck, Phleger & Harrison, LLP, 12390 El Camino Real, San Diego, CA 92130 (US).

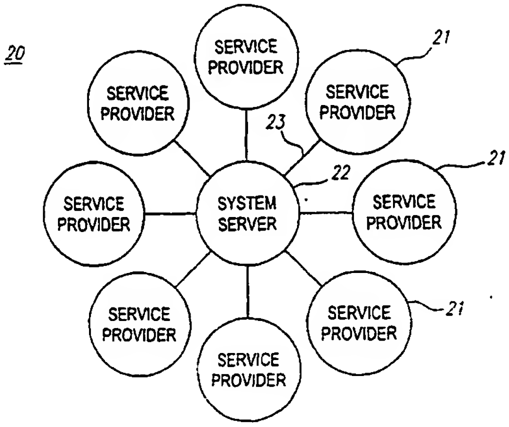
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR ANONYMOUS TRANSACTIONS AND DISGUISED MAILINGS



WO 01/48628 A2

(57) Abstract: An automated system for the confirmed efficient authentication of an anonymous subscriber's profile data. The system is comprised of software/hardware interface to facilitate centralized access and exchange to easily and inexpensively allow the confirmed authentication of subscriber profiles of customers wishing to blind their transactions, while maintaining current services. In one aspect the system allows a subscriber to anonymously accomplish credit card transaction without associating any aspect of the transaction with any information associated with the true identity of the subscriber. The system also allows disguised mailings, including a service that provides a portable private mailing code for mailing physical items to the subscriber without disclosing the subscriber's actual address. A private mail administration center (PMAC) registers each subscriber, assigns a unique private mailing code to the subscriber, and maps the mailing code to the subscriber's physical delivery address. A private mail mapping center (PMMC) receives the mapping information from the PMAC and provides a controlled-access, secure interface to shippers, such as the United Parcel Service, for accessing the subscriber's delivery address, enabling direct shipment of the physical items to the subscriber.

(15) Information about Correction:
see PCT Gazette No. 42/2001 of 18 October 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

System and Method for Anonymous Transactions and Disguised Mailings

BACKGROUND OF THE INVENTION

Field of the Invention

The disclosed invention relates to the field of electronic transactions and particularly to processes and devices for facilitating the anonymous authentication of customer profile information to an authorized requester, and a system and method for protecting the privacy of customers when ordering merchandise by mail by not having to reveal their address to the merchant and/or shipper.

Description of the Related Art

As computing capacity increases and data handling and storage become easier and less expensive, information databases are assembled to host a myriad of transactional information. This information, which may be gathered from a number of sources, is stored, categorized and sold. A prime information target is the retail transaction. Membership cards, club cards and credit cards which link a transaction to an individual's database, reveal the purchase, the time of day of the purchase and the retail outlet. This information is then tied to a demographic which is sold to the direct marketing industry. In many cases these databases actually invade a person's privacy and are almost transparent to the unwitting consumer.

It is particularly easy to assemble such information when the transactions involve a third party. For example, a credit card company or bank can use the information it acquires in the course of credit or bank card transactions to determine the spending habits of particular customers. The credit card company or bank can then either use that information in its own business or make that information available to others. The consequences of the availability of information about an individual's spending habits range from the annoying to the serious. At a minimum, the individual receives more targeted junk mail than he or she might otherwise; more seriously, the same information that is used to target the individual for junk mail can be used to target the individual for activity which is tantamount to harassment.

One way an individual can avoid this problem is to pay for everything with bearer notes such as cash, since nothing on a bank note indicates who its owner is or was. This same property, however, makes cash fungible for both the owner and the thief. It is both easy to lose and easy to negotiate. For these reasons, few people desire to carry a large amount of cash. One way of solving this difficulty is to use electronic cash, as described in David Chaum, "Security without Identification: Transaction Systems to make Big Brother Obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030-144, October, 1985. When electronic cash is used in an automated transaction, a purchase cannot be associated with a customer. The scheme, however, may be insecure against fraud; see Steven H. Low, et al., "Collusion in a Multi-Party Communications Protocol for Anonymous Credit Cards" submitted to *IEEE/A* CM 50 Transactions on Networking. In addition, since the electronic cash is given to a customer, a means is needed to prevent the individual from duplicating and spending it over and over again.

What is needed is a way of performing transactions that has the convenience and safety of card transactions, such as credit card transactions, and the anonymity of cash transactions. It would therefore be advantageous to have a safe, secure, easy to use system to facilitate the confirmed authentication of customer related identity and business information between a service provider and a customer.

In addition, it is often desirable to protect the identity of consumers when ordering merchandise over the telephone or the Internet or by any other means, when such merchandise is to be shipped to the residence or business of the consumer. The problem is, that the consumer must ordinarily give a proper mailing address to the merchant in order to receive the shipped goods.

One solution to this problem is to use post office boxes. However, this solution is often expensive, inconvenient and often requires the use of the consumers real name rather than an alias name. Therefore, what is needed is a system and method to protect the identity of consumers names and addresses when ordering merchandise that is to be shipped to the consumer.

SUMMARY OF THE INVENTION

The disclosed system and method concerns a means by which a service provider or merchant is an information requester authenticating customer-related information and/or records which reside in a secure, offline database without revealing the true identity of the customer. As recognized by the present invention, it is desirable that during or subsequent to a customer transaction, the service provider or authentication requester is able to authenticate the existence of the customer without having the true identity of the customer revealed.

The present invention provides an automated, inexpensive system and method for the confirmed request, processing and confirmed transfer of anonymous customer or subscriber related authentication among service providers and/or information requesters. The system is preferably comprised of a software and hardware system to facilitate centralized offline customer identity and business information authentication, while maintaining the anonymity of the customer. This advantageously allows a service provider or information requester to easily and inexpensively authenticate customer-related business information without the true identity of the customer being revealed to the service provider. Thus, a benefit of the present invention is that the actual transaction is not associated with the true identity or demographics of the customer.

Another benefit of the present invention is that a highly efficient method is provided for requesting, processing, and anonymously authenticating customer or subscriber related identification and business information between the service provider or information requester and the secure, central, database repository. In one aspect of the present invention, this comprises an information hub which includes an interactive server and a database. For example, in one embodiment, the database contains a lookup table which blinds the database from the server. Preferably, the coded or addressed anonymous customer identification confirmation or authentication system of the present invention employs an offline central consumer information database or repository, in communication with service providers or information requesters. The system and method provide for the processing and authentication of requested, specifically identified customer profiles, without identifying the true identity of the customer, and without revealing any business or transaction information to the service provider or information requester. In a preferred embodiment, the authenticity of the information requester is verified prior to responding. Thus, one feature of the present invention is that there is a blinding or "bunkering" of any attempt by unauthorized information requesters to cross check against a known transaction to match the alias of the customer or subscriber with the true identity of the customer or subscriber.

Another advantage of the present invention is that a multiplicity of service providers or information requesters having a system authorization code, can electronically request, process and confirm the validity of an anonymous customer's information and/or records. This can be done, for example, from a secure data repository by means of a hardware/software system. Preferably, the hardware/software system is comprised of an offline database and a central server comprising an information processing hub. In this example embodiment, the information processing hub communicates with each service provider or information requester via a communication link.

A feature of the present invention is that a confirmed authentication of uniquely identified and stored information between an authorized requester and the database repository is triggered by the use of a unique, assigned alias identifier. For example, the requested subscriber or customer records and/or business information are uniquely identified by means of an alias identification of the customer, which can be alphanumeric, digital, analog or the like. In one embodiment the system can authenticate the existence of the customer alias as relating to the true identity of an individual subscriber. In another embodiment, authenticated coded triggers are used to release a predetermined portion of the data including, for example, the true identity of the subscriber, to an information requester having authorization for that clearance. In accordance with this embodiment, preferably the information is encrypted. In one aspect, an alpha numeric code is used to identify files within the uniquely addressed customer information profiles. In a preferred embodiment, the system of the present invention confirms requests for authentication to maintain the integrity of the system and the anonymity of the subscriber or customer. In another embodiment the authentication is protected by encryption and a digital signature of the information requester or by use of an authentication code such as a PIN or the like.

In a preferred embodiment, personal or business records and/or information related to a particular subscriber maintained within the offline database can include at least part of at least one subscriber's profile. In one aspect subscriber profiles consist of the subscriber's physical address, social security number, credit limits, e-mail address, and the like. In accordance with a preferred embodiment contemplated herein, a single centralized offline database or repository is provided in communication with a central processing server. For example, the central processing server acts as a "gatekeeper" to maintain the secrecy of the customer's true identity. In another embodiment, a plurality of servers communicate with the service providers and in turn with a central server in a multi-tiered system.

In another aspect of the present invention, a computer implemented method is disclosed for providing authentication to an authorized information requester. For example, the information requester may be provided with authentication of the existence of coded, uniquely identified personal business type records and/or information relating to a particular anonymous subscriber or customer. In a preferred embodiment, the records or information are contained in a "blinded" offline database that communicates with each authorized information requester by means of a central processing server. The method, for example, may be accomplished by the subscriber information requester initially generating an authorized formatted request for authentication of the uniquely identified records and/or information related to a particular anonymous subscriber or customer using an alias that retains the anonymity of the subscriber or customer. The method also includes transmitting the request to a confirming central processing server with access to an offline database via the communication link. Additionally, the method includes receiving the formatted request, authenticating the authorization of the information requester and confirming receipt of the formatted request by the central system database. The method also includes processing the request of the subscriber or information requester by blinded communication with the database, generating a formatted response in the database authenticating the alias or denying the alias, transmitting the response, and formatting a server response to the service provider or information requester via the communication link.

In one examplary embodiment, the formatted response to the subscriber or information requester can comprise a denial of the request, an authentication or an authenticated informational compliance. Additionally, the informational compliance can be full or partial. In a preferred embodiment, the requester is logged into the central server. For example, if the information requester is not authorized to address the offline database, the identification of the customer or subscriber is blocked and the information requester is denied further communication. In this example, such a formatted response is a denial of authentication.

In accordance with a preferred aspect of the invention, a medium is provided which contains a unique identification that is either anonymous or an alias with respect to the true identity of the subscriber and/or customer. For example, the medium can be in the form of a standard plastic card with a magnetic strip containing the encoded information or alias information or it can be in the form of a smart card that has an encoded chip. Alternatively, in addition to the card, there may be an alias I.D., such as a picture I.D., that authenticates the anonymous code for the user. In an example embodiment, a personal identification number ("PIN") can be used such that the user of the medium would be required to enter a PIN on a keypad or the like, to authenticate the anonymous code. A benefit in these examples is that the user of the medium remains totally anonymous to the service provider or requester. Also in the above examples, the service provider authenticates the transaction by means of an electronic connection such as telephone wires or the Internet to one or more centrally based processing servers in communication with the offline database as previously described.

In accordance with another embodiment, the medium can be a credit card issued by, for example, American Express, VISA or MasterCard. For example, the service provider requests verification of the anonymous user through a central processing server to an offline database. Next, an authentication code response is sent to the service provider and information located in the look up table, such as the purchase, the purchaser and the amount, is then encrypted and transferred to a credit card provider bank to be posted to the subscriber's account.

In accordance with another embodiment, a "Kid Card" is a credit or debit card that makes limited purchasing power available to children. Preferably, the transactions performed with the Kid Card are anonymous and the products available for purchase with the Kid Card are subject to parental control. In one example embodiment, children are guided through the shopping experience by the Web pages supplied by the hosting entity.

For example, in one embodiment, the transactions performed with the Kid Card are anonymous. A child that purchases an item over the Internet, for example, can use the Kid Card to pay for the item. When real-time approval is sought by the entity processing the transaction, rather than using true identity data to authenticate the transaction, an alias set of information is used. This alias set of information is compared to an offline secure database that compares the alias information to the true identity data and authenticates the transaction. In this example, the true identity of the purchaser is thus never compromised and therefore never available to the processing company for inclusion on a demographic list or the like.

In addition, the present invention provides a means for consumers to have mail or merchandise ordered via telephone, the Internet, or any other means, to be shipped to their business or residence, without having to reveal their true address to the shipper and/or merchant. The mail or merchandise is shipped to a mailing code and re-labeled with the true address of the consumer sometime after shipment by the sender. As described in detail below, this is preferably, but not necessarily, accomplished in combination with an anonymous transaction system (such as any of those described herein), using one of at least two possible methods. The first method involves shipping the packages to a temporary location where the true address is re-labeled on behalf of the consumer using information from the offline database. A private facility administers the database, registers the customers, and assigns the mail codes to the registered customers before this anonymous mailing and re-labeling service is started.

In a second embodiment, the shipping company pre-registers with the private facility that administers the database and receives access to a secure network connection with the offline-database. The shipping company in possession of a package labeled with a mailing code sends a valid authorization request, including the mailing code, to the offline database through the secure network connection. The private facility verifies the authorization request and returns the true address of the customer to the shipping company, thus enabling the shipping company to deliver the package directly to the customer. Preferably, this process is automated and is implemented using wireless technology while the package is in transit.

In a related aspect, the present invention provides a means for a person or entity to receive mail or parcels from a sender (e.g., a merchant) anonymously. For example, the contact with the sender can be via telephone, the Internet, or any other means. The sending may, but need not be, in connection with a commercial transaction (e.g., a sale or purchase) or involve the shipping of ordered goods as described above. Thus, the item can be shipped to their business or residence, without having to reveal their true address to the shipper and/or merchant. The mail or parcel is shipped to a mailing code and re-labeled with the true address of the consumer sometime after shipment by the sender. In cases where the item is sent as part of a commercial transaction, this is preferably accomplished in combination with the anonymous transaction system. The method preferably uses one of the two methods described above.

In embodiments of the various aspects described herein involving anonymous or disguised mailing or shipping, the mailing code assigned can include limited non-identifying information. For example, the code may be formatted similarly to a zip code, in that the code or a portion of the code corresponds to a geographic area or political subdivision. Thus, for example, the code may correspond to a postal zip code area or group of zip code areas, a city, a county, a state, or other suitable area. Also, the re-addressing may be physical or electronic or a combination of the two. Thus, for example, the re-addressing may be by affixing or otherwise physically associating, a legible address (with or without name), by affixing or otherwise physically associating a machine readable form of the address, e.g., a bar-coded or magnetic strip address, by affixing or otherwise physically associating a translatable, machine-readable address (e.g., that is translated within a special or general purpose computer), by affixing or otherwise physically associating an access identifier enabling electronic access to sufficient identifying information (preferably on screen or other display) for delivery to the customer or other intended recipient, or by using the mailing code to allow (preferably with additional authorization code) remote electronic access to specific delivery information, preferably during the course of a delivery run. For example, delivery information may be displayed on a computer in a delivery truck or on a hand-held computer. Remote access may be by any suitable means, e.g., by telephone (preferably mobile telephone) and/or via satellite communications link, which may involve internet transmission.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 is an example of a schematic view of an information flow model that can be used in accordance with one embodiment of the present invention.

Figure 2 is an example of a schematic view of an information flow model that can be used with one embodiment of the present invention having a central processing server and an offline database.

Figure 3 is a block diagram depicting one example of a method that can be used to create a new account.

Figure 4 depicts an example of a process that can be used to book a Primary account from part 1 of the application in accordance with one embodiment of the present invention.

Figure 5 depicts an example of a process that can be used to process part 2 of the application in accordance with one embodiment of the present invention.

Figure 6A depicts an example of bunker operations for application processing in accordance with one embodiment of the present invention.

Figure 6B depicts one example embodiment of an acquisition process in accordance with one embodiment of the present invention.

Figure 6C depicts an example application process that can be used in one embodiment of the present invention.

Figure 7 depicts an example of a method that can be used to establish an Alias account as an extension of an existing account.

Figure 8A is an example of a method that can be used to perform maintenance in accordance with one embodiment of the present invention.

Figure 8B is an example of some account management and maintenance tasks in accordance with one embodiment of the present invention.

Figure 8C is an example of a collection method that can be used in accordance with one embodiment of the present invention.

Figure 9A depicts a process that can be used to replace the alias name and address with the real name and address before the statement is printed in accordance with one embodiment of the present invention.

Figure 9B depicts an example of a statement process that can be used in accordance with one embodiment of the present invention.

Figure 9C depicts one example of a plastics process that can be used to emboss alias credit cards in accordance with one embodiment of the present invention.

Figure 10 depicts a method that can be used for payment of the Alias account in accordance with one embodiment of the present invention.

Figure 11A is an example that depicts one method that can be used by the bunker to support mail redirection in accordance with one embodiment of the present invention.

Figure 11B is one example of a method that can be used for mail redirection from both the host and bunker perspective in accordance with one embodiment of the present invention.

Figure 12 depicts an example process flow which shows the type of information flowing in and out of the Bunker receiving point, the Host and the Bunker in accordance with one embodiment of the present invention.

Figure 13 is an example of database tables that can be used to implement the bunker database in accordance with one embodiment of the present invention.

Figure 14 is a schematic diagram that depicts one embodiment of the disguised mailing feature in accordance with one embodiment of the present invention.

Figure 15 is a flowchart depicting methods that can be used to implement the disguised mailing feature in accordance with an embodiment of the present invention.

Figure 16 is a flowchart depicting methods that can be used to implement the disguised mailing feature in accordance with an embodiment of the present invention.

Figure 17 illustrates information flow during package delivery using the private anonymous mailing service of the present invention.

Figure 18 is a flowchart of the customer registration process used in the private anonymous mailing service of the present invention.

Figure 19 is a flowchart of the merchandize shipment process in accordance with the private anonymous mailing service of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In accordance with a preferred embodiment in operation, an information hub housing a central server receives a request for authentication from a service provider or information requester. In this example embodiment, the central server verifies that the service provider or information requester is authorized to obtain authentication for the transaction or the requested information from the database. For example, upon verification of the validity of the request, the central server queries the database for authentication of the anonymous customer. The database contains, for example, a lookup table that links the anonymous identification of the medium card holder, for example, a credit card holder, to the true identity of the card holder. In this example embodiment, the lookup table functions a barrier between the system traffic and the stored identity information.

Continuing with the example, if the information requested matches the search in the lookup table, a verification response is generated by the central server to authenticate the transaction. This could be used, for example, with telephone cards, frequent flyer club cards, grocery store cards and the like.

After reading this description, it will become apparent to one of ordinary skill in the art how to implement the invention in alternative embodiments and alternative applications. Moreover, other examples for blinding interaction and transaction will readily come to mind, once the inventive aspect of the instant invention is understood. Although the instant system can be used to blind customer profiles from a service provider for a number of applications, credit card transactions will be used as a specific example for ease of understanding. As such, this detailed description of a preferred and alternative embodiments should not be construed to limit the scope or breadth of the present invention.

Subscriber

For purposes herein, a "Subscriber" is an entity who subscribes to a transaction based service and whose data is in the offline database. A "Service Provider or Information Requester" is an entity with which the particular Subscriber is consummating a transaction. Service Providers could be, for example, local retailers, banks, travel agencies and the like. "Subscriber D" is an alias system identifier that can be used as an alias or a code to uniquely identify a particular Subscriber and its records. "Subscriber Profile" or "Service Profile" means customer-related business information and/or records such as a particular Subscriber's financial information, or address. "Subscriber Related Business Information Request" is a request from a Service Provider for authentication of all or part of a particular Subscriber Profile or Service Profile. The Profile preferably contains readable system code allowing the system to verify the requester is on the system. A "Subscriber Related Business Information Request Response" is a response to a Subscriber Related Business Information Request. For example, the Response could be a listing of all or part of a particular Service Profile, an authentication of a Subscriber's identity, or a denial of such information. In a preferred embodiment, the Response is encrypted. A Subscriber Related Business Information Request Response can also include a "Transaction Authorization" or "Confirmation Request" such as used in the credit card industry.

Turning to FIGURE 1, there is shown an example of a schematic that can be used for the alias method and system 20 of the instant invention. In a preferred embodiment, the alias method and system 20 comprises a number of Service Providers or Information Requesters 21, each communicating with a system server/database 22 by means of a pre-existing communication link 23, such as the public telephone system. For example, the system server/database 22 can be a centralized information hub, having a pre-existing communication link 23 for the purposes of receiving, authenticating and transmitting information to Service Providers 21. In an alternative embodiment, the central information hub may comprise more than one physical element. For example, a multi-tiered server system (not shown) may be practical in some applications. Furthermore, a public communications system is not necessary to link the system server database 22 to the Service Providers 21. The communications link 23 may alternatively be a private leased line, a local area network, cable TV network, or the Internet. In a preferred embodiment, the system server/database 22 comprises a server and an offline database as more fully described below in relation to FIG. 2.

In a preferred embodiment, a Subscriber Profile data and/or authentication is relayed to a requesting Service Provider 21 through a system server/database 22, in computer accessible code, via a communications link 23. In one example, the information flow is virtually instantaneous, and the response information puts the necessary information in the hands of the Service Provider or Information Requester 21. This information is preferably delivered in a usable form, expediting the transaction.

Turning to FIG. 2 there is shown an example of an information flow diagram that can be used in of one aspect of the inventive alias method and system 20. In the example depicted by FIG. 2, the transfer of a Subscriber's authentication or Subscriber Profile information between the Service Provider or Information Requester and the offline centralized database is shown. Preferably, the system server is accessible to all Service Providers 21. For example, the Service Providers 21 can access the System Server 22 by merely addressing the alias customer information profile by means of the Service Provider's identification through the communication link.

As further shown in FIG. 2, the example system 20 comprises an authorized Service Provider 24, a System Server 26, an offline database 28, and an interconnecting communications link 30. Preferably, the communications link 30 connects the Service Provider 24 and database 28 with the server 26. Additionally, the diagram in FIG. 2 schematically represents an example of the data flow within the system 20. In this example, the processes represent execution steps for creating, transferring and confirming information between Service Provider 24, server 26, and offline database 28. Preferably, this communication takes place by means of communications link 30.

Generation of Request for Subscriber Authentication or Information

In a preferred embodiment, Service Provider or Information Requester 24, by means of unit process 33, generates a Subscriber Related Business Information Request 32. For example, the request is generated in a specified format and includes an informational header. This header includes, for example, the Subscriber's alias, PIN or other anonymous inquiry keys and information. Additionally, the header may include address information and a formatted message portion comprised of, for example, the date, time, and amount of the transaction.

In a preferred embodiment, the data used to generate the Subscriber Related Business Information Request 32 can be provided in more than one way. A first example of a method for creating the Subscriber Related Business Information Request 32 is by using an application Graphical User Interface, preferably written in Java. In one embodiment, the Graphical User Interface provides the user with input fields for all elements of the Subscriber Related Business Information Request 32, including input fields for the Service Provider 24. Additionally, the Graphical User Interface can perform input validations, convert the input data into a binary stream using Java serialization, and store the document. For example, the document can be stored in binary object form in the Service Provider or Information Requester's 24 relational database.

A second example of a method for creating the Subscriber Related Business Information Request 32 is through the use of the Client Integration Subsystem. In a preferred embodiment, the Client Integration Subsystem is a configurable set of services and infrastructure. These services can be written, for example, in the C++ and Java programming languages. Furthermore, the services can, for example, allow an organization to "plug-in" their existing systems to automatically generate Subscriber Related Business Information Request 32. For example, the Request 32 could seek the coded information in a credit card transaction that authorizes a merchant's request and identifies the return path.

In both example embodiments, the resulting document is stored in the Service Provider or Information Requester's 24 relational database coupled with additional document information. For example, such information could include date and time stamps, document state information, creating user identification, and the like. Furthermore, this information could be linked to a particular Subscriber Related Business Information Request 32 and simultaneously stored along with the Subscriber Related Business Information Request 32. Preferably, the date and time stamps are used to determine whether the request is sent and received within the industry allotted time period. This, for example, would prevent hacking through the use of different requester locations attempting to obtain client Subscriber Related Business Information in the offline database 28. Additionally, the user identification information is preferably used by the System Server 26 and the offline database 28 to help verify the validity of the Subscriber Related Business Information Request 32. This can be done, for example, by determining that the Subscriber Related Business Information Request 32 was sent by an authorized Service Provider or information Requester 24.

In this example, when the Subscriber Related Business Information Request 32 is completed by entering the necessary data, it is marked as ready to be sent. Conversely, if the Subscriber Related Business Information Request 32 is not completed, for example, due to missing data, it is marked for review and stored until the Subscriber Related Business Information Request 32 data is entered into the Subscriber Related Business Information Request 32. Preferably, this prevents overriding the system by not having a complete request. This is important, for example, when service information provider or information requesters 24 are given security codes allowing access to differing information and/or levels of information.

Send Subscriber Business Information Request from Service Provider or Information Requester to the System Server

In a preferred embodiment, once created, the Subscriber Related Business Information Request 32 is prepared to be sent to the System Server 26 by means of unit process 34 via communications link 30. An example of the aspects of unit process 34 include application of the digital signature, data encryption, alias and attaching the routing information. For example, the Subscriber Related Business Information Request 32 carrying the alias identifier is encrypted by an encrypting service. In one example embodiment, the encrypting service utilizes Pretty Good Privacy encryption with a private key based on the system server's 26 public key. In one embodiment, an online service can be used or alternatively, the software can be downloaded from www.MIT.edu. for inclusion in process 34. Continuing the example, the document is digitally signed using the Service Provider's 24 private key. Preferably, this private key has been previously configured by the system administrator.

In one embodiment, the Subscriber Related Business Information Request 32 is sent to the server 26 using communication link 30. Various systems can be used to connect the Service Provider or Information Requester 24 to the System Server 26. For example, the message can be sent either via X400 protocol or using a virtual private network protocol. Preferably, the choice is based on the configuration implemented by the generating entity's system administrator, based on system requirements for response times and cost of implementation. In both example methods, a lookup of the server 26 destination address in the Service Provider or Information Requester's 24 database is performed. Preferably, the process 34 appends the appropriate routing information for the transmission type used by the generating entity system. A fully qualified Internet address is an example of appropriate routing information. Finally, the data is preferably sent over an existing communication system such as the Internet or a Virtual Private Network.

Receipt of Subscriber Related Business Information Request by System Server

In a preferred embodiment, the Subscriber Related Business Information Request 32 is received by server 26 from Service Provider or Information Requester 24. For example, this can be accomplished by means of unit process 36 via communications link 30. In one embodiment, the system is activated by data being received. Preferably, unit process 36 includes steps for receiving the message, authenticating the signature on the message and responding to the sender if the signature is valid. For example, upon receipt of a Subscriber Related Business Information Request 32, the server 26 first logs the receipt and then authenticates the digital signature. Within process 36, in the same example, an interim file representation of the document is created, after extracting the document from the transport mechanism and stripping off header information. The file is then stored in a system-defined, file system directory. Subsequently, the document digital signature is verified using the Pretty Good Privacy signature authentication service based on the sender's public key, which is retrieved via the previously configured information in the Pretty Good Privacy security database. Continuing the example, if the signature is authentic, the Subscriber Related Business Information Request 32 is decrypted using the Pretty Good Privacy decryption software and stored. Preferably, a verification of receipt message 38 (shown in dotted lines) is sent back to Service Provider or Information Requester 24 via the communication link 30. In a preferred embodiment, the Service Provider or Information Requester 24 verifies the sender as the System Server 26.

In an example embodiment, the validity of the Subscriber Related Business Information Request 32 is based on several criteria. Preferably, if the Subscriber Related Business Information Request 32 is not authentic, the Request 32 is not honored. For example, in one embodiment, the invalid Request 32 is first returned to the Service Provider or Information Requester 24 via the Communications Link 30. Then, a message is sent noting the receipt of an invalid Subscriber Related Business Information Request 32.. Furthermore, receipt of the invalid Subscriber Related Business Information Request 32 is logged by the System Server 26. Preferably, the address of the invalid Service Provider or Information Requester 24 is "blocked" from the system 20 and the information pertaining to the unauthorized Service Provider or Requester 24 is maintained in the system 20 for future reference.

Processing of the Subscriber Business Information Request for Subscriber by System Server

In a preferred embodiment, valid Subscriber Related Business Information Requests 32, received by the System Server 26, are processed in accordance with unit process 40. For example, the processing includes decrypting the message and preparing the message for forwarding to the offline database 28. Preferably, a message header is appended to the message and a document timer is activated to track the time until the System Server 26 receives a request response from the offline database 28.

In an alternative embodiment, to process the Subscriber Related Business Information Request 32 in accordance with 40, the System Server 26 preferably records receipt of the Subscriber Related Business Information Request 32 into the System Server's 26 relational database. In this same embodiment, the Subscriber Related Business Information Request 32 is marked as received by the System Server 26. Furthermore, the Server 26 can also be configured to execute certain user defined operations which are triggered during this processing depending upon the nature of the Subscriber Related Business Information Request 32 as further described below. For example, if the request is a credit card transaction, certain information may be forwarded to the issuing bank after database manipulation as further described below.

In one embodiment, the document file is read in by the Server's 26 document handier, decrypted, and the document is then stored in the Server 26. For example, a document handler rules engine is used to process the document in accordance with unit process 40. Based on a user defined rules set, preferably stored in an ASCII text file, a rules agenda is created based on the contents of the document. In this example, the rules engine matches patterns in the rules conditions with the document and executes actions associated with the conditions. Examples of actions include updating database tables, modifying/transforming the document header information, and adding additional/alternative document routing instructions. Preferably, a timer is activated by storing a new record with Subscriber Related Business Information Request 32 information in the timer table.

Send the Subscriber Business Request for Subscriber Profile from the System Server to the Database

In a preferred embodiment, subscriber Related Business Information Requests 32, thus processed, is ready to be forwarded to offline database 28 by means of unit process 42 via communication link 30. An example embodiment of unit process 42 includes the steps of encrypting the message, digitally signing the message, and sending the message to the offline database 28. Preferably, the functions required to prepare a document for forwarding are based on the type of Service Provider 24 from which the Subscriber Related Business information Request 32 is received. For example, if offline database 28 has authority and access to the data required to respond to the Subscriber Related Business Information Requests 32, it can create a Subscriber Related Business Information Request Response.

Receipt of the Subscriber Business Information Request for Subscriber Information from System Server by Offline Database

In one embodiment, the offline database 28 receives, logs, and authenticates the Subscriber Related Business Information Request 32. For example, in unit process 44, the offline database 28 receives the message, the signature on the message is authenticated and a response is sent to the System Server 26 if the signature is valid. In this manner only the Server 26 can access the offline database 28.

In a preferred embodiment, after receipt of the Subscriber Related Business Information Request 32, the information is processed in accordance with unit process 44. For example, process 44 creates an interim file representation of the document after extracting the document from the transport mechanism and stripping off header information. Here, the priority code is interpreted so that the appropriate information from the lookup table can be retrieved. Continuing the example, the Subscriber Related Business information Request 32 is stored and the appropriate customer related information is coupled with the document header. Preferably, The file is stored in a system-defined file system directory. Subsequently, the digital signature is verified using the Pretty Good Privacy signature authentication service based on the sender's public key, which is retrieved via previously configured information in the Pretty Good Privacy security database. If the signature is authentic, the document is decrypted using the Pretty Good Privacy decryption software based on the server's private key data.

In one embodiment, once the document is decrypted, the header information is separated from the Subscriber Related Business Information Request 32 and the Subscriber Related Business Information Request document 32 is stored. For example, a message 38 (shown in phantom) acknowledging the receipt of the Subscriber Related Business Information Request 32 is then sent by the offline database 28 to the Server 26 via communications link 30. Preferably, Erroneous Subscriber Related Business Information Request 32 receipts are logged and the Server 26 is notified via message 38. In this manner only requests from server 26 are accepted for processing.

Processing of the Subscriber Business Information Request for Subscriber Information and Generation of Response by Offline Database

In an alternative embodiment, once the Subscriber Related Business Information Request 32 is processed as set out above in unit process 44 by offline database 28 it is processed in accordance with unit process 46. An example of the method steps within unit process 46 includes: the Subscriber Related Business Information Request 32 is decrypted, the document is stored into the offline database 28 and the Subscriber Related Business Information Request Response 47 is created. For example, the offline database 28 formats the data into a document message and the offline database 28 appends reader information such as routing and document type to the message. Additionally, the subscriber Related Business Information Request 32 is stored in the offline database 28.

When the Subscriber Related Business information Request 32 has been processed, the Offline Database 28 responds. For example, the Offline Database 28 sends a Subscriber Related Business Information Request Response 47 back to the Service Provider or Information Requester 24 through the System Server 26 via communications link 30. Preferably, the Subscriber Related Business Information Request Response 47 is generated in accordance with unit process 46. In one example, the Subscriber Related Business Information Request Response 47 is prepared using an application Graphical User Interface preferably written in Java. The Graphical User Interface, for example, provides the user with input fields for all elements of the Subscriber Related Business Information Request Response 47, including input fields for the Service Provider or Information Requester 24. Preferably, the Graphical User Interface performs input validations, converts the input data into a binary stream using Java serialization, and stores the document in binary object form into the offline database's 28 relational database.

In a preferred embodiment, the document is stored into the offline database's 28 relational database. For example, the document may be stored with additional document information such as date and time stamps, document state information, creating user identification and the like which are linked to a particular Subscriber Related Business Information Request Response 47. Preferably, the document state information is used by the system to determine whether the Subscriber Related Business Information Request Response 47 is ready to be transferred to the System Server 26. Additionally, the user identification information is used by the System Server 26 to help verify the validity of the Subscriber Related Business Information Request Response 47 by determining that the Subscriber Related Business Information Request Response 47 was sent by offline database 28 or an entity having access to the subscriber information and authority to disseminate authentication or information.

In one embodiment, when the Subscriber Related Business Information Request Response 47 is completed by entering the necessary data, it is marked as ready to be sent. Conversely, if the Subscriber Related Business Information Request Response 47 is not completed due to missing data, it is marked for review and stored until the Subscriber Related Business Information Request Response 47 data is entered into the Subscriber Related Business Information Request Response 47. Preferably, a message is sent to the Server 26 requesting additional information be placed in the database 28 to fill the request.

Send the Response to the Request for Subscriber Information to System Server from Offline Database

In a preferred embodiment, after Subscriber Related Business Information Requests Response 47, has been processed, it is ready to be forwarded to System Server 26 by means of unit process 48 via communication link 30. For example, within unit process 48, Subscriber Related Business Information Requests Response 47 is encrypted, digitally signed, and sent to the Server 26. After processing, the Subscriber Related Business Information Request Response 47 is preferably stored in the relational database coupled with additional information such as date and time stamps, and user identification.

Receipt of the Response to the Subscriber Information Request by System Server from Offline Database

In one embodiment, after the Subscriber Related Business Information Request Response 47 is received by the System Server 26, it is handled in accordance with unit process 50. For example, within unit process 50, the system server receives the Subscriber Related Business Information Requests Response 47, the signature on the Subscriber Related Business Information Requests Response 47 is authenticated, and a response 38 is sent to the offline database 28 if the signature is valid. Preferably, the Subscriber Related Business Information Request Response 47 is acknowledged by message 38 to the offline database 28 via link 30 and its receipt is logged.

Continuing the example, the Subscriber Related Business Information Request Response 47 is processed by Server 26. An example of this processing includes authentication of the Subscriber Related Business Information Request Response 47 and validation of the intended Service Provider 24 address. Additionally, the receipt event is logged. Preferably, the document is decrypted as above described and checked against existing Subscriber Related Business Information Request 32 for a match. For example, Subscriber Related Business Information Request Response 47 match errors and destination errors are logged and notifications sent back to the offline database 28. Furthermore, the respective unit process 50 creates an interim file representation of the document after extracting the document from the transport mechanism and stripping off header information. In this same example, the file is stored in a system-defined file system directory. The document digital signature is then verified using signature authentication service based on the sender's key. Preferably, if the signature is authentic, an acknowledgment message 38 is created and sent back to the Offline Database 28 via the same communication mechanism that the document was received. In one method, the converted response is stored in the server's 26 persistent storage mechanism.

Processing the Response to the Subscriber Information Request by System Server

In an alternative embodiment, after the Subscriber Related Business Information Request Response 47 response is received by Server 26, it is processed as shown by unit process 52. Such processing, for example, includes storing the document, logging its receipt and managing the timers associated with the original request. For example, within unit process 52, Subscriber Related Business Information Requests Response 47 is decrypted, an ID is matched against the initial request sent, the message is stored into the System Server 26 database, the document timer is deactivated, the Subscriber Related Business Information Requests Response 47 is prepared for forwarding to the requesting Service Provider 24 and a message header for sending Subscriber Related Business Information Requests Response 47 to the requesting Service Provider 24 is appended. Preferably, the Subscriber Related Business Information Request Response 47 receipt is logged and the document state is set to "complete." Such a setting indicates that the

Subscriber Related Business Information Request Response 47 is ready, for example, to be encrypted, signed, and forwarded to the Service Provider or Information Requester 24, as represented by unit process 54..

In a preferred embodiment, the document file is read in by the Server's 26 document handler process and the document is then stored in the Server 26. The Document Handler Rules Engine is then activated to process the document. For example, a rules agenda is created based on the contents of the document. The rules engine matches patterns in the rules conditions with the document and executes actions associated with the conditions. The rules match the Subscriber Related Business Information Request Response 47 by document identifier information with the Subscriber Related Business Information Request 32. Preferably, the system timer that was created when the document was originally received by the server 24 is deleted from the server timer table. Subsequently, in this example, the destination for the Subscriber Related Business Information Request Response 47 is validated and any erroneous Subscriber Related Business Information Request Responses 47 are logged. Preferably, The Document Handler process modifies the Subscriber Related Business Information Request Response 47 header information for document transmission status and stores the information to the database.

Send Response to Subscriber Information Request from System Server to Service Provider

In one example embodiment, the Subscriber Related Business Information Requests Response 47 is sent to the Service Provider 24 using the communication link 30 in accordance with unit process 54. For example, within unit process 54, the Subscriber Related Business Information Requests Response 47 is encrypted, digitally signed, and then sent to the Service Provider 24. Additionally, the system appends the appropriate routing information for the transmission type used by the Service Provider 24. Furthermore, acknowledgment of receipt is received via 38 and logged. Preferably, match and destination error notifications are received and logged, corrections are made and the response re-sent if necessary.

Receipt of the Response to the Subscriber Information Request by Service Provider

In an example embodiment, upon receipt of the Subscriber Related Business Information Request Response 47, the Service Provider or Information Requester 24 authenticates the System Server 26 as the sender and logs the receipt of the Subscriber Related Business Information Request Response 47 in accordance with unit process 56. For example, within unit process 56, Subscriber Related Business Information Request Response 47 is received, the digital signature is authenticated, and a response 38 is sent to the System Server 26 if the signature is valid. Additionally, the digital signature is verified and the Subscriber Related Business Information Request Response 47 is matched against the Subscriber Related Business Information Request 32. Preferably, the Subscriber Related Business Information Request Response 47 is processed in a manner similar to unit process 46 in accordance with unit process 58.

Service Provider Processing of the Response to the Subscriber Information Request

In an alternative embodiment, the Service Provider or Information Requester 24 processes the Subscriber Related Business Information Request Response 47 in unit process 58. For example, within unit process 58 Subscriber Related Business Information Request Response 47 is decrypted and matched to the Subscriber Related Business Information Requests 32 stored in the requesting Service Provider's 24 database. Furthermore, the document status is set to complete or rejected depending on the response data sent in the Subscriber Related Business Information Requests Response 47 by the offline database 28. Preferably, the completion of this step is the termination of the process.

In a preferred embodiment, a log entry is made into the system server database recording information about the document reception process. For example, the document state is set to complete by the document processor of Server 26 by updating the document header in the database. Preferably, a trigger is fired to perform a system defined service upon document completion. Triggers, for example, can perform actions such as sending a user-defined message to a socket, storing data in another database, performing communications and the like. In this manner transaction data can preferably be sent to, for example, an issuing bank.

The Systems Server and Offline Database

An example of the system server/offline database architecture consists of six subsystems: process control subsystem, communication subsystem, document processing subsystem, security subsystem, user interface subsystem and a data handling and storage subsystem.

Process Control Subsystem

A descriptive example of the process control subsystem includes a system that invokes and controls the other custom and commercial software that make up the system server. This subsystem, for example, is able to automatically restart erroneously terminated processes and logs such terminations for later analysis. Preferably, users are able to configure the process control subsystem to take additional actions when a process terminates.

Communication Subsystem

An example of the communication subsystem is further comprised of an X400 agent and/or virtual private network communication agent. Preferably, this subsystem uses either agent to send documents out of the system server to external recipients, and relies on a fully qualified Internet address for routing.

For example, the communication subsystem's message receiving functions include determining how to route a message to its recipient, and accepting and transferring mail from and to intermediate agents. Additionally, address interpretation and transformation into a compatible format is handled by the communication subsystem. The communication subsystem also implements special actions indicated by the message header such as verifying delivery. For example, when message delivery cannot be done, the communication subsystem queues messages, or reroutes documents with erroneous addresses, as required. To send messages to a recipient, the communication subsystem determines the recipient's pre-existing public communication system host, then initiates a transfer protocol session with the host. Preferably, an unsuccessfully transferred message is queued for later delivery.

In an embodiment where the System Server 26 functions as a routing hub for the system, the communication subsystem receives and processes all incoming document transfer protocol sessions from client systems. For example, outbound documents are packaged and sent to the communication agent for processing. Additionally, the communication subsystem automatically processes received messages by first authenticating, then decrypting, and then sending the message to the document processing subsystem. In one embodiment, the communication subsystem places a time stamp on each message that when compared with the message status indicates when a message has not been successfully delivered. Unsuccessfully sent messages are preferably resent a predetermined number of times according to preset communications subsystem parameters.

Document Processing Subsystem

In a preferred embodiment, the document processing subsystem processes all messages received into the System Server 26. For example, this subsystem can be responsible for message parsing, message storage, Subscriber Related Business Information Request processing, Subscriber Related Business Information Request Response processing, message routing and message timers. Preferably, messages are processed in the order in which they are received and deleted after successful processing.

In a preferred embodiment, a message is logged into the activity log upon reception and then parsed. For example, the message parser divides the message into two parts: header and message data. Message type information contained in the header determines which type of action the system server should take with the message data. After parsing, the message data is stored. Preferably, the message data is stored according to message type and the message header is logged. For example, a Subscriber Related Business Information Request is stored in a Subscriber Related Business Information Request table; and a Subscriber Related Business Information Request Response is stored in a Subscriber Related Business Information Request Response table. In an alternative embodiment, table entries are crossed referenced, and transmission verification messages and the status of the corresponding message are logged.

In an example embodiment, after the message is stored, the Subscriber Related Business Information Request 32 is processed. For example, the first step in processing a Subscriber Related Business Information Request 32 is to log the event. Then the name of the service provider 24 is extracted and the service provider's address is obtained from a lookup table. The Subscriber Related Business Information Request 32 is then sent to the offline database 28. Preferably, the Subscriber Related Business Information Request 32 is marked as sent when a return receipt is received. In alternative embodiments, Subscriber Related Business Information Requests 32 can be in any of four states based on responses from the offline database 28: pending, sending, inactive, or completed.

In a preferred embodiment, after the Subscriber Related Business Information Request 47 is processed and sent to the service provider, the Subscriber Related Business Information Request Response 47 is processed after it is received from the service provider. For example, when a Subscriber Related Business information Request Response 47 is received by the document processing subsystem, the corresponding Subscriber Related Business Information Request identification number is located and the Subscriber Related Business Information Request status is checked. The Subscriber Related Business Information Request Response 47 is marked as invalid if the Subscriber Related Business Information Request 47 is not pending. Preferably, Document status is updated when the Subscriber Related Business Information Request Response 47 is processed, forwarded to the requesting Service Provider or Information Requester 24 and stored into the system.

In a preferred embodiment, a message's time in the document processing system is tracked by a timer. In one example, default events are set to occur at pre-set times. Preferably, such default events include setting a message's status to a certain value if no response has been received or to send the message again if no return receipt is received.

Security Subsystem

In an alternative embodiment, the security subsystem primarily secures four areas: system data and file access, the relational database, the system administrative user interfaces and data and messages. For example, system data and file access to the offline database 28 is protected by a user identification string that allows access to only the owner. Preferably, access to the relational database is controlled through a data owner's user identification string and password, and no access privileges are granted to any other user. Additionally in this example, the system administration user interfaces and data are protected by another set of user identification numbers and passwords. Preferably, users can not gain access to the system administration user interfaces and data through other databases.

In one embodiment, messages are secured by encryption and a digital signature. For example, commercial security software does the encrypting and decrypting, message authentication, and digital signature verification. Software specifically designed to secure document transmissions using Public Key Cryptography is preferred. In alternative embodiments, Public Keys can be manually transferred between system/client administrators via e-mail or disk/tape. Preferably, key transfers are authenticated by verifying the digital signature of the sent document.

Furthermore, all messages preferably receive a digital signature based on the private key of the sending system. For example, upon receipt, the digital signature of a message is automatically verified. Messages that fail digital signature verification are not processed, but rather are stored and the failure noted in the automated activity log. Preferably, the sender is not notified when a message fails verification. This, for example, is to prevent attacks from hostile systems.

User Interface Subsystem

In a preferred embodiment, the user interface subsystem allows a system administrator to add or delete service providers, add or update message routing information and monitor system activity. Preferably, the interface is accessed through Java software applets which can be executed within a web browser, such as Netscape Navigator or as a stand alone application.

Data Storage Subsystem

In one embodiment, offline database system data is stored in the commercial relational database. For example, the offline database system uses a database access and storage facility implemented using embedded structured query language in the user application processes and Java Database Connectivity. In an alternative embodiment, the Unix file system can be used to store system data.

It will be realized by the skilled artisan that many transactional applications lend themselves to the anonymity provided by the instant invention. Accordingly, in one aspect, particular service providers or Information Requesters have security codes and/or priority codes which allow them access to some, if not all, of the information contained in the offline database. This, for example, would be the situation with an issuing bank with a particular credit card that has been issued to a Subscriber in the anonymous system and various pieces of information with regard to, for example, financial status of the Subscriber are required in accordance with the Agreement between the Subscriber and the bank. Preferably, this information flow is handled by the server as set forth above after authentication of the total transaction.

It will be realized that alternative embodiments of the system in accordance with the instant invention can provide some or all of the information contained in the database to a particular Service Provider or Information Requester depending upon the degree of anonymity, the position of the Service Provider or Information Requester, and the access codes/alias identifiers of the system. Thus, in accordance with one aspect of the invention, no information is allowed to any Service Provider or Information Requester and in that aspect the system has the capability of providing authentication or authorization code for a particular transaction completely devoid of any subscriber information. Further, it will be realized that particular embodiments will allow grocery cards and club cards such as frequent flyer and the like (which are primarily involved in gathering demographic information with regard to purchasers)to be "blinded" by the use of the instant invention.

In accordance with the instant invention, it will be realized that, for example, a number or series of aliases or codes such as personal identification numbers, and the like can be used in association with the medium to reduce risk of unauthorized use of the medium. In accordance with a preferred embodiment, security codes may be issued to the Subscriber such that one or more of the security codes must be used depending on the magnitude of the transaction. Further, it will be realized that although plastic cards are an easy medium in which to embed alias identification, alternative embodiments may employ other mediums such as electronic transfer medium, smart cards, chips, and the like. Thus, as long as the medium can maintain and contain at least one set of alias identifiers that can be recognized by the system, any medium can be used in accordance with this invention. For example, codes on keypads and even fingerprints would be acceptable identification to trigger the system.

Example Embodiments

The following is an example of one specific embodiment of the present invention. While this particular example embodiment of the improved system and method for anonymous transactions is fully capable of attaining the above described features and benefits of the invention, it is to be understood that this example embodiment represents a presently preferred embodiment of the invention and, as such, is merely a representative of the subject matter that is broadly contemplated by the present invention. It is further to be understood that the scope of the present invention fully encompasses embodiments other than the example embodiments presented herein. Accordingly the examples presented herein should not be construed to limit the scope or breadth of the present invention.

In the example embodiment presented herein, an account is provided that can be used while maintaining the anonymity of its user. An offline database, also referred to as a "processing bunker" allows for two separate accounts to be established for an individual. In a preferred embodiment, the bunker is the only place that contains information that associates an account used for establishing a line of credit to the alias account used to protect the identity of the cardholder.

Below are some definitions used below that are useful for describing this example embodiment of the present invention.

Primary account - the account applied for that has all the accurate information about the cardholder and is used to establish a line of credit.

Shadow account or Alias account - an account that uses an alias name and alias address to protect the anonymity of the cardholder. It is preferably attached to a Primary account through the bunker. In the examples and some of the Figures presented herein, this account is also referred to as a "Casper" account.

Normal Account - a standard credit-card account that has nothing to do with the Primary and Shadow accounts of the present invention.

Bunker - The process that supports linking of the Primary and Shadow accounts together. The bunker may be in a separate facility, or in an existing data center depending on the amount of separation desired in each specific implementation of the present invention.

Credit-Card Processing System - As described in detail below, the present invention can be used with existing credit-card processing systems. In some of the Figures and examples below, an existing credit card processing system is also referred to as "FDR".

The bunker is preferably constructed to provide a standalone source for synchronizing information between the Primary account and the Shadow account. It also provides services for properly addressing communications to the cardholder. These functions are preferably driven from a database containing information on both accounts. In one embodiment, the bunker has no public network connections outside of the building. In this fashion, the present invention provides an extremely secure environment for the matching information.

This example embodiment can be used with existing credit-card processing models with minimal intrusion. The remainder of this example describes the bunker functionality and its interaction with a typical existing credit-card processing model.

In the example embodiment, a new product is provided that protects the identity of the cardholder. It allows the establishment of a line of credit that is split across two accounts. The two accounts are referred to as the Primary account and the Shadow account. The Primary account is the account booked using factual information provided on an application. The Shadow account is the account booked using information from the Primary account with an Alias name and address.

In one embodiment, the Primary account is a standard credit account that can be used like a traditional credit card. The credit line for the card is established as some portion of the credit line approved during application processing. The remaining portion is assigned to the Alias card. In this example embodiment, two cards are used because of possible restrictions that may be placed upon the use of the Alias card. For example, the Alias card may be restricted in places where proof of ID is required, such as for hotel, airline and rental car reservations.

ACQUISITION

In one embodiment, the acquisition of Shadow accounts can be accomplished in two ways. The first is through new account solicitation.. For a new account, a new application is completed and a new credit card account and an Alias account is created. The second way relates to associating an Alias card account with an existing credit card account already on file. The following example describes both of these scenarios.

New Accounts. Figure 3 is a block diagram depicting one example of a method that can be used to create a new account. As shown, in one embodiment, a new account acquisition is accomplished using a two-part application 60. Both parts 62 and 64 of the application 60 have a document tracking number (shown as "123" in Figure 3). The document tracking number is used in this example embodiment to construct a relationship between the Primary credit card account and the Shadow account. Preferably, the document tracking number is unique. Each part of the application 62 and 64 is sent to a different destination as shown by Figure 3.

Specifically, part 1 of the application 62 is mailed to the issuer's application processor. Part 2 of the application 64 is mailed to a receiving point for the bunker. Preferably, each of the application parts 62 and 64 has only the document tracking number ("123") in common. This number is used in the bunker to create the relationship between the Primary account and the Shadow account.

In a preferred embodiment, the document tracking number is captured in a master file when the application is processed. In this fashion, the document tracking number can be passed to the bunker after the account is booked. In one embodiment, bunker receiving is not in the bunker location itself, but in a location where part 2 of the application is actually received and the Alias name and document tracking number is captured for input into the bunker.

Thus, key points for protecting the anonymity of the account holder include sending part 1 of the application 62 to a different location than part 2 of the application 64, and the only common information between all parts is the document tracking number on the application 60.

In a preferred embodiment of the present invention, rules for processing the application 60 follow the issuer's standard process. Such a process may already be in existence for processing normal credit-card accounts and the like. For example, credit bureau reports are requested and the account is scored to determine eligibility. Preferably, the only special requirements are that the credit line being established is split between the two accounts, the Primary and the Shadow account, and the capturing of the document tracking number from the application so that it can be later passed to the bunker for matching with the Alias.

Figure 4 depicts an example of a process that can be used to book a Primary account from part 1 of the application 62. As shown, part 1 of the application 62 is mailed from the cardholder. A data entry terminal 72 is used to enter the information from the application 62 into a computer system, such as the IBM mainframe 74 shown in Figure 4. If the application is not approved, standard rejection letters are typically sent back to the applicant. However, if the application is approved, it will be booked. Information related to the new Primary account is then stored in the account file 76. This information includes the actual name and address of the cardholder but does not include the alias information.

Figure 5 depicts an example of a process that can be used to process part 2 of the application 64 in accordance with one embodiment of the present invention. Part 2 of the application 64 is handled separately from part 1. This part 64 is used to assign an alias name to the Shadow account when it is built. Part 2 of the application 64 contains the alias name and the document tracking number that matches the number on part 1 of the application 62. As shown, a data entry operator using a data entry application on a personal computer (PC) or the like 80 captures the information. In one embodiment, the application on the PC 80 creates a file that is stored on removable media 82 and transferred on a daily or other periodic basis to the bunker.

An example of bunker operations for application processing is shown in figure 6A. The bunker receives a file 82 comprising part 2 alias information as described above. This information is used as input to a matching database process or application program 88. Alias information is posted to the data store 90 using the document tracking number. If the document tracking number is already on file, a check is made to determine if the alias information has already been posted. If it has not, then a new account record is created and added to a file that is sent to the host (not shown) for posting. If the alias information has already been posed, then an error is reported.

It is important to note that in one embodiment, the above-described process takes information for a cycle and uses it to create input for the next cycle. That is, if an account is approved before the day's cycle kicks off, the new account is created during the night cycle and the information for the bunker is extracted from files created during that cycle. The file will then be hand-carried to the bunker for processing. This input to the bunker is then processed and the new Alias accounts and other account updates are loaded into files that will be transferred by hand back to the account processing facility for the next night's cycle.

Details of one example embodiment of an acquisition process is shown in Figure 6B. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s). IT is noted that in these example, the Shadow and/or Alias account is also referred to as the "Casper" Account. These details expand on the principles described above and provide a specific implementation of one example embodiment. It should be noted that these details are for exemplary purposes only and should not be construed to limit the scope and breadth of the present invention, which could be implemented using alternative means.

For an existing account, the credit line has to be increased and/or split to accommodate both the cards on approval. The host will receive non-mon (non-monetary transaction) from the bunker for updating the credit line of the primary account. Also the output is merged with that of the Casper specific output.

An example of a process including typical inputs and outputs that can be used to match the Primary and Alias accounts for acquisition is as follows

Input:

- Document Tracking Number and/or the primary account number from the Account file.

Output:

- Corresponding Alias Account details from the Temporary Database (See Figure 6B).

Process:

Query the Temporary Database for the given Document tracking number or Primary Account Number or the like, to obtain its Alias account details.

Figure 6C depicts an application process as described above for a specific example embodiment. It is noted that in Figure 6C, a three part application is referenced rather than a two part application as described above. However, the third part of the example application is merely a record for the application card-holder in this example. It should be noted that in a preferred embodiment, at least a two part application is used as described in detail above with respect to Figures 3-5.

The following is a summary of an example acquisition process, for a new and existing account, as can be seen in Figures 6B and 6C.

Input:

New account

- A 2-part form is filled up.
- The 2 parts have a common Document Tracking Number.
- Part 1 of the Application, which is mailed to the Issuer's Processor, is treated just as a normal account.
- Tape from the bunker (non-mon to the mainframe) for creating new Alias accounts.
- Non-mons from the bunker requesting the update of Primary account status and credit line.

Existing account

- Part 2 of the application is filled up. The Primary account number is supplied to the bunker as the Part 1 information.

- A non-mon from the bunker requesting the Part 1 details.
- Tape from the bunker (non-mon to the mainframe) for creating new Casper accounts.
- Non-mons from the Bunker requesting the update of Primary account status and credit line.

Output:

- Account file that goes to the bunker.
- Creation of Alias or Casper and Primary Accounts (in case of new account)

Process:

- Rules for processing the application (both part 1 and part 2) preferably follow the Issuer's standard process.
- Update the master file.
- Capture the newly booked primary accounts to the *Account File.*
- This Account File will is written to tape or other removable media that is to be sent to the bunker. Proper formatting of the data is typically required. This is actually a non-mon sent to the bunker from the host.

Bunker updates its database using the Account File 76 and generates an Alias Account File that is sent to the host through a tape or other removable media. These records will be posted in the next day's Cycle as a new Account Processing Facility. This is a non-mon from the bunker to the host.

Existing Accounts. Figure 7 depicts an example of a method that can be used to establish an Alias account as an extension of an existing account. The cardholder completes an application 60 or request for the Alias account similar to the new account process as described above. This application also has two parts, 62 and 64. One part 62 goes to the issuer 104 and the other part 103 goes to the bunker receiving point (not shown). Typically, the issuer 104 receives the application and performs a credit investigation for approval of the Alias account. If the research is successful and an Alias card is to be issued, the credit line is increased to accommodate both cards. A new entry screen is created that is used to send the account information to the bunker 108, as shown by 105. In this fashion, the process works in a similar fashion as the new account process described above.

In one embodiment, the account information is pulled from the master file either using an account dump or some other means of collecting the information that needs to be passed to the bunker. The file that is created will go to the bunker as illustrated above in Figure 6 and the Alias account is created to be booked during the next cycle.

Example Bunker Processing. Typically, two data sources provide input for construction of matching database records. One source is the part 2 information 64 containing the Alias name and document tracking number. The second is account information 76 created by processes on the host. Standard date and time tracking of information is performed for management of the data. Reports are typically generated to insure that processing works as desired and standard audit trails are established.

A data entry program is created that can be used to capture part 2 information 62. This information can then be transmitted to the bunker or hand carried into the bunker depending on location of the data entry personnel. Regardless, this is an offline process that requires a bulk transfer on a daily or other periodic basis. An additional data entry is provided to the issuer for doing approval of Alias accounts associated with an existing account. This should connect to a local server at the credit-card processing facility so that it can collect the account information needed for the bunker process.

Example Host Processing. New account information is collected for those accounts that are being created as part of the Alias credit-card product, as shown by 106. The information is then formatted for transfer to the bunker, as shown by 110. Account information is also collected from the system for those existing accounts that are having an associated Alias account. The information is preferably pulled from an account dump and then formatted for the bunker.

Example of creating a new Alias account

The following example summarizes an example process in accordance with the present invention that can be used create an Alias account. This example process is from the perspective of the bunker.

Example Input:

- The Alias Name file containing the part two of the new account requisition form.
- The account file for the Primary account, for which the Alias Account is to be created.

Example Output:

- Creation of the matching database.
- Creation of a non-mon to create an Alias Account on the Cardholder Master File. This non-monetary transaction will be an input to the next day's cycle to the host.

Example Process:

- Retrieve the information from the Alias Name file entered by the operator at the Bunker Receiving and store it in the Temporary Database.
- For a new account, retrieve the information from the Account file present in the Bunker Receiving and store it in the Temporary Database.
- For existing account, for each Primary Account Number on Part 2, send a non-mon to the host to obtain the Part 1 details for the same. Store these details in Temporary Database.
- For each Alias Account, fetch the corresponding details from the Temporary Database for either the Document Tracking Number or the Primary Account Number.
- Select an account number for the new Alias account from the Accounts Block Table. If the end of the account block has reached, generate an error log for the operator.

- If no error, generate an alias address for the new Alias account.
- Add a new record to the Matching Database which has information like Primary account number, Alias account number and the Alias Box number and other information.
- Enter the date and time in LastUpdateDateAndTime field of Matching Database. This is for maintaining the audit log.
- Add a record to the Mail Redirection Database containing Alias Box number, Real Name and Address and Alias Name and Address of the Cardholder.
- Create a non-monetary transaction and the Alias accounts file, for the host to create a new Alias account.
- Create a non-mon for the host to update the status and Credit line of the Primary account.

Maintenance

Daily maintenance tapes are preferably produced containing updates made to the Primary and Shadow accounts. These updates are preferably used to insure that the matching database 92 in the bunker is accurate.. Updates that require processing include name and address changes as well as changes in available credit.

The updates may be extracted from an existing file 120 such as shown in Figure 8A. This file 120 is a daily record of all non-mon's that were posted. Typical changes required by existing credit-processing systems include additional steps as shown in Figure 8. For example, one step 122 takes the data from the daily update file 120 and creates a file for those records associated with Alias accounts. The file is then be transferred to the bunker for processing 124. Outputs from the bunker, if any, are updates that are input into the next day's cycle, as shown by steps 128 and 126.

Examples of maintenance tasks are as follows:

- *Request for a change in Alias Name, Address or the Credit Line for Alias Account.* These changes are preferably performed only on the bunker side. If Host updates the master file and sends a non-mon to the bunker, the bunker preferably sends a non-mon back to the Host to rollback the changes made to the master file. If these changes were first done on the bunker side, then the bunker sends a non-mon to the host to update the Alias account on the host database. Examples of some account management and maintenance tasks are shown in Figure 8B.

- *Request to terminate the Alias account by the Cardholder.* In this example, the bunker receives a request from the cardholder to terminate the Alias account. In response, the bunker sends a non-mon to notify the host about the same. It also sends non-mons to update the status and credit line of Primary account.

- In case of the Primary account, the change of name and address is transferred to the bunker through a file/tape, which the bunker uses to update the database with the new real name and real address.

- *Request for a change in the credit line for Primary account.* This process is shown in Figure 8B. The Host treats this change as a normal maintenance change for a Normal account. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s). Host updates the credit line for the Primary account and send a non-mon to the bunker to make changes accordingly. The bunker then updates the credit line for the Primary and Alias account as per the Credit Ratio. The bunker will send a non-mon back to the host to the update the Alias account credit line as a part of the next day's cycle. It is noted that the communications between the bunker and the credit processing system is through removable media or a secure network connection, as described above. These connections are depicted in Figure 8B by the reference numerals 127 and 129.

Collections

One method that can be used to process and account that goes into collection is presented follows.

(a) The Host through a non-mon informs the Bunker about the account going into collection.

(b) Bunker generates non-mons to do an AT (Account Transfer) of the Alias account to the Primary account *i.e.* terminate the Alias account and update the Primary account.

(c) The bunker generates non-mons for putting the Primary account into the working queue and for updating the status of the Primary account.

(d) The host sends a confirmation for AT to the Bunker. The Bunker would then update the corresponding flags on its database.

A detailed specific embodiment of a collection method is presented in Figure 8C. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s).

When an Alias or its Primary account goes into collections the bunker receives notification so that appropriate actions can be taken. The normal procedure when a Alias account goes delinquent will be for the bunker to generate non-mon's combining the two accounts into the Primary account. This will allow the collectors to have access to the information they need to work the account as well as provide proper reporting. The Alias account is preferably closed to prevent its use. In one example, during the nightly collections process, a file is created that contains all the Alias accounts that have gone into collections. Preferably, an agreement with the cardholder specifies that either account going into collections is terms for termination of the Alias account.

Example Bunker Processing. Those Alias accounts that become delinquent and require collections are passed to the bunker. The appropriate non-mons will be generated to combine the two accounts. The non-mons are then added to the file to be transmitted for the next night's cycle.

Example Host Processing. In one example, a special queue is set up to catch the accounts that need to be sent to the bunker. This queue can then be captured and sent to the bunker to be processed. Once the changes have been made to the account they will be placed in a working queue.

Communications

Statements and mailers sent to the cardholder of an Alias account are preferably ether redirected by placing a mailing label over the alias-mailing information or by changing the name and address of the mail piece before it is mailed. By placing a label over the mailing information can create an item that can compromise the anonymity of the cardholder. That is, all the information (Real name, Alias name, Real address and alias address) is available on the mail piece. Accordingly, a preferred method is to change the name and the address before it prints. In this fashion, the only information that is exposed is the real name and address and any other information that is on the mail piece.

For all communications, such as Statements, Plastics and PIN mailers for the Alias Accounts, the host preferably prints information to a file. This file is transferred to the bunker, which replaces the alias name and address with the actual name and address.

Figure 9A depicts a process that can be used to replace the alias name and address to the real name and address before the statement is printed. As shown, to correctly address the statement, the records for Alias accounts are moved into a separate file. This file is then carried to the bunker where the correct name and addresses are changed 136. When this is complete the output tape is then returned to the credit-processing printing facility, where a monthly statement 138 is printed.

Bunker Processing Example. Typically, the bunker will receive three different files for mail processing. The standard statement file is received for Alias accounts. On the statement the alias name and address is overlaid wherever it appears on the statement and the payment coupon. The same is true on the Plastic and PIN mailers. Once the files have been passed they are transmitted back to the credit-processor to be printed and mailed.

Host Processing Example. The statements for the Alias accounts are preferably treated as if they are being printed by an external print shop. The print files for the Alias accounts are separated and sent to the bunker for processing. When the bunker is finished they are returned and sent to output services for normal printing.

Typically, card and PIN Mailers have strict security requirements placed on them. Generally, an association must certify any facility that handles these items. Anyone that handles these items other than the cardholder and the postal system typically must typically be certified. To make this process as streamline and cost effective as possible a preferred approach is to make use of a facility that has already been certified.

In this example, the bunker provides an extract file to such a facility that can be used to change the name and address information on the Alias accounts mailers to be the real name and address. The name on the card will be the alias name. This will allow the cards to be mailed to the correct address. The account number on the mailer will be the matching one on the card so quality assurance of the plastics will still be able to insure that the process is working correctly.

An detailed example of a specific implementation of a statement process is shown in FIG. 9B. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s).

Figure 9C depicts and example of a plastics process that can be used to emboss alias credit cards. Preferably, there is no major impact on the embossing part of the process. One or more of the input files are preferably flagged to identify the Plastics/Cards associated with an Alias account. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s).

For the Alias Cards/Plastics, the alias name and address is replaced with the actual ones in order to send the Card to the correct destination. Thus, the host receives this information from the Bunker before sending it for embossing, as shown in Figure 9C.

Payment

Payments are to be handled in a normal manner, that is a manner that is used for normal or standard credit-card accounts. This means that the cardholder will be required to make payment to each account that has a balance. Preferably, there will be no transfer of balance from one account to another to reduce complexity of the system. In one embodiment, the cardholder receives a payment coupon with each statement that will allow them to make payment for that account.

Making payment by check on the alias account poses little chance of compromising the account relationship. Figure 10 depicts a method that can be used for payment of the Alias account. A payment coupon is sent with the monthly statement 150. Only the payment coupon is sent in with the payment 151. The payment coupon has the real name and address on it. This was performed as part of the re-labeling process in the bunker before the statement was mailed, as described above. When the payment arrives at the payment-processing center 152 the payment is credited to the account based on the account number presented on the payment coupon. There are no additional bunker and host processing requirements for this process.

Mail Services

In a preferred embodiment, mail redirection is not the responsibility of the bunker. However, the bunker is typically required to support it. Figure 11A is an example that depicts one method that can be used by the bunker to support mail redirection. As shown, to support mail outside of the bunker, a separate database 162 is provided that can be queried using, for example, the box number assigned to the Alias account. The query returns the correct name and address of to be used. This database 162 is preferably outside of the bunker and is made available via a secure network connection for use by those doing mail redirection.

In one example, the information included in the address subset database 162 is as follows:

- Alias Box Number (Key)
- Real Name
- Real Address

The box number is preferably be unique. Further, a special zip code is preferably acquired from the post office to trigger this special handling. The zip code should be assigned to the facility that handles the manual re-labeling process for those items that are captured through special processing. The box number will be generated in the bunker and assigned when the Alias account is built.

Example Bunker Processing. Two extract databases are typically built daily containing information for creating mailing labels. Both extracts contain the real name and address for mailing purposes. One extract is keyed by the box number in the alias address and the other uses the real account number as its key. These two databases can then be loaded on another machine or transmitted to the re-mail facility for use in creating labels.

A detailed example of a specific implementation of a mail redirection process from both the host and bunker perspective is shown in FIG. 11B. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s).

Figure 12 is a block diagram that depicts an example process flow which shows the type of information flowing in and out of the Bunker receiving point, the Host and the Bunker. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s).

EXAMPLE DATA BASE DESIGN

Figure 13 is an example of database tables that can be used to implement one specific embodiment of the bunker database in accordance with one embodiment of the present invention. This figure is self-explanatory as would be apparent to persons skilled in the relevant art(s). The following tables include details of the various fields shown in the example data base design shown in Figure 13.

It should be noted that this is just one example of database fields that can be used in one example embodiment of the present invention.

- **Temporary Database 184**

Sr. No.	Field Name	Data type	Description
1.	IsNew	Boolean	This field will decide if the Alias account to be created is for a new or an existing Primary account.
2.	DocumentTracking Number	AlphaNumeric	This field will contain the document tracking number for a new primary account for which a Alias account has to be created.
3.	AliasName	AlphaNumeric	This field will contain the alias name for the Alias account. The name will be selected from the available names list.
4.	AliasAddress	AlphaNumeric	This field will contain the alias address for its Alias account. It will be generated by a special algorithm.
5.	PrimaryAccountNumber	AlphaNumeric	This field will contain the account number for any primary account for which a Alias account has to be created.
6.	RealName	AlphaNumeric	This field will contain the real name for its primary account.
7.	RealAddress	AlphaNumeric	This field will contain the real address for its primary account.
8.	IssuerCode	AlphaNumeric	This field will contain the issuer code for the Cardholder.
9.	IsAccountCreated	Boolean	This flag if true, will indicate that the Alias account has been created.

Notes:

- Fields 2, 3 and 4 comprise the Part 2 of the account requisition form.
- Fields 5, 6, and 7 comprise the Part 1 of the account requisition form.
- Flag IsNew decides if the Primary account is new or existing.

- In case of new account, any part of the requisition form may come first at the bunker. Whichever part arrives first at the Bunker will be stored in the database. The other part of the requisition form will be entered in the database, using the DocumentTrackingNumber mentioned on that part.
- In case of existing Primary account, Part 2 has to arrive at the bunker, before Part 1. The PrimaryAccountNumber, will be one of the fields in Part 2, which will be used to obtain Part 1 details from the host. When the Part 1 arrives later, the Temporary Database will be queried based on the PrimaryAccountNumber, so that the appropriate record can be updated.

- **Matching Database 180**

Sr. No.	Field Name	Data type	Description
1 .	PrimaryAccountNumber	AlphaNumeric	This field will contain the account number for any primary account that has a Alias account.
2.	AliasAccountNumber	AlphaNumeric	This field will contain the account number for the Alias account for the given Primary account number.
3.	AliasBoxNumber	Numeric	This field will contain the alias box number for its Alias account. This number will be generated by a special algorithm.
4.	ActivePrimaryAccount	Boolean	This flag if set, indicates that the primary account is active and if reset, indicates that it is not.
5.	ActiveAliasAccount	Boolean	This flag if set, indicates that the Alias account is active and if reset, indicates that it is not.
6.	ProcessingRequired	Boolean	This flag if set, indicates that a non-mon has been generated for this account. Hence it need not be considered again for sending to the host in the next cycle.
7.	LastUpdateDateTime	DateAndTimeStamp	This field indicates the date and time of the last update done on this account.

8.	PrimaryCreditLine	Numeric	This field will contain the current value of the maximum available credit for the Primary account.
9.	AliasCreditline	Numeric	This field will contain the current value of the maximum available credit for the Alias account.
10.	IssuerCode	AlphaNumeric	This field will contain the issuer code for the Cardholder.
11.	StartDate	DateStamp	This field will contain the date on which the Alias account was created.
12.	EndDate	DateStamp	This field will contain the date on which the Alias account was terminated.

- **Mail Redirection Database 182**

Sr. No.	Field Name	Data type	Description
	AliasBoxNumber	Numeric	This field will contain the alias box number for its Alias account. This number will be generated by a special algorithm.
2.	PrimaryAccountNumber	AlphaNumeric	This field will contain the Primary account number for the Alias account.
3.	RealName	AlphaNumeric	This field will contain the real name for its primary account.
4.	RealAddress	AlphaNumeric	This field will contain the real address for its primary account.
5.	AliasName	AlphaNumeric	This field will contain the alias name for the current Alias account.
6.	AliasAddress	AlphaNumeric	This field will contain the alias address for its Alias account.

- **Account Block Database 186**

Sr. No.	**Field Name**	**Data type**	**Description**
1.	IssuerCode	AlphaNumeric	This field will contain the issuer code.
2.	IssuerName	Alpha	This field will contain the issuer name.
3.	StartBlock	Numeric	This field will contain the start of the account block for the current Issuer.
4.	EndBlock	Numeric	This field will contain the end of the account block for the current Issuer.

5.	LastAccountN umber	Numeric	This field will contain the last account number used for the current Issuer.

- **Issuer Database 188**

Sr. No.	Field Name	Data type	Description
	IssuerCode	AlphaNumeric	This field will contain the issuer code.
2.	PrimaryCreditProportion	Numeric	This field will store the percentage of the Primary credit line of a cardholder.
3.	AliasCreditProportion	Numeric	This field will store the percentage of the Alias credit line of a cardholder.
4.	ActiveDate	DateStamp	This file will indicate the date from which the change of Credit line has to come in effect.

Additional Notes pertaining to the example embodiment of the Database described above.

- Document Tracking Number (DTN) is preferably unique to the issuer and the Cardholder.

- In case of new account, the DTN is preferably captured to pass on to the bunker for matching with the alias. The DTN will be stored in some miscellaneous field on the host database.

- In case of existing account, the Primary account number should be captured. The DTN will typically not be stored.

- The host database will have a method for distinguishing the primary accounts having Alias accounts from those which do not have (regular accounts).

- The bunker can request for an account dump based on the Primary account number through a non-mon. Other possible ways could be to delete and re-create an existing account or do an account transfer.

- The Alias name file would just have the DTN and the alias name. Other details like the mother's maiden name etc. would be taken from the Part 1 of the application or from the existing account.

- Part two of the application would be keyed in through a user interface on the bunker side. The issuer would process part one of the application.

- The credit investigation will be done on the host side, before starting the bunker processing.

- Credit line is split between the 2 accounts by the bunker (assumed to be pre-defined, either cardholder specific or issuer specific.)

- The bunker would have the information about the split in the credit line stored in a control file. For Primary and Alias Card/Plastic, embossing comes separately. Separate card carriers will be used to mail them.

- The Temporary Database on the bunker side will contain only such records for which Alias accounts are to be created.

- When a Alias account goes into collections it is terminated and its details are combined into the Primary account, which is then sent for collections. The decision of terminating the Primary account will be taken by the issuer.

- Updates to a Alias account may include change of alias address or a request to stop the Alias account by the user.

- The Alias Box number and the special zip code in the alias address cannot be modified by the cardholder. The bunker process, in some critical conditions can modify it.

- In case a credit limit changes in the Alias account, it would be transferred to the bunker since a Alias account is treated as a normal account by the host. The bunker will then change the limit back to the original limit.

- Credit limit of a Alias Account can be changed only by changing the limit of its Primary Account. The bunker would then re-adjust the limit of the Alias account and create non-mons for updating both on the host side.

- The bunker would issue the Alias account number by selecting a number from the block of available numbers.

- If a Cardholder wishes to update the real address, it will first be updated on the host and then the same change will be incorporated in the Mail Redirection Database on the bunker side.

- Audit log would be generated for all the file transfers on bunker as well as host to ensure that all files sent by one are received by the other.

- If a primary account no longer has a Alias account, the database on the host will be modified accordingly, to reflect the same.

- The Matching Database will have a field to indicate the last modification date/time for every account.

- The Temporary Database on the bunker side will be purged after creating the Alias accounts in it.

- There would be flags to indicate the active/inactive statuses of Primary and Alias accounts on the bunker side. Whenever any account is to be terminated the corresponding flag would be set to false implying inactive. Additionally, there would be a flag to indicate if a non-mon has been generated for that inactive account.

- If one account goes into collections, the bunker will be informed about the same. Bunker would then generate a non-mon to do an account transfer of Alias account to Primary account. The host would then put the Primary account into the working queue.

- The format of transferring the files from host to bunker can be anything but from bunker to host, it has to be in the format which the host can understand without changes to the existing system.

- The issues to be considered while creating the Temporary Database are following: The Part 1 of the application may come before the part 2 of the application. Therefore Part 1 of the application needs to be stored in the Temporary Database. The Part 1 may be received much later than Part 2, even after weeks. Part 1 may not be received at all.

- The statements printed for the Alias account would have only the name and address replaced.

- Out of the three I-files only the file containing the embossing details will be affected in case of embossing.

- In case of the statement generation activity, the Alias Account number will not be replaced along with the alias name, address. The acquisition function will generate an error log to inform the operator that the account block for a particular issuer is over. So to be able to create a new Alias account, the operator should increase the block limit.

- The name and the alias address will also be stored in the Bunker database. This is required, because if a request comes from the host to change the alias name and address, there has to be some way of finding the old name and address to compare it with. Since the request has come from the host, the host database already has the new values. Hence to restore the old values, they need to be stored in the *Mail Redirection Database.*

- After deactivating the Alias account, the host should send an Account Transfer confirmation to the bunker.

- If a cardholder wants a Alias account for the second time, *i.e.* after having closed the previous Alias account, a new record will be added to the *Mail Redirection Database.*

- In case of changes to the alias name and address from the operator, a new record will be added to the *Mail Redirection Database.*

- There would be background process or a scheduler running on the bunker side to compare the system date with the ActiveDate in the Issuer Database. This scheduler will trigger the bunker processing based on the system date in addition to the Bunker Receiving.

Kid Card Example Embodiment

The following is a description that depicts one example embodiment of the present invention. While this particular Kid Card embodiment is fully capable of attaining the above described features and benefits of the present invention, it is to be understood that the Kid Card embodiment represents a presently preferred embodiment of the invention and, as such, is merely a representative of the subject matter that is broadly contemplated by the present invention. It is further to be understood that the scope of the present invention fully encompasses embodiments other than the Kid Card and that the scope of the present invention is not limited by the following example embodiment.

In a preferred embodiment, the Kid Card is a credit or debit card that makes limited purchasing power available to children. Preferably, the transactions performed with the Kid Card are anonymous, and the products available for purchase with the Kid Card are subject to parental control. In one embodiment, children are guided through the shopping experience by the Web pages supplied by the hosting entity.

Anonymity

In a preferred embodiment, the transactions performed with the Kid Card are anonymous. For example, a child that purchases an item over the Internet uses the Kid Card to pay for the item. When real time approval is sought by the entity processing the transaction, rather than using true identity data to authenticate the transaction, an alias set of information is used as described above. This alias set of information is compared to an offline secure database in the bunker that compares the alias information to the true identity data and authenticates the transaction. In this example, the true identity of the purchaser is thus never compromised and therefore never available to the processing company for inclusion on a demographic list.

Parental Control

In one embodiment, parents can put restrictions on the types of items that the Kid Card may purchase. For example, the authenticating database might be configured to allow the purchase of only Type1 and Type2 items. Thus, if a child attempted to purchase a Type3 item such as adult content material or a Tommy Gun, the transaction would be denied.

Alternatively, the parental control can take the form of restrictions on the products that are available for purchase. For example, a group of parents who have created a Web page can offer the Kid Card. In this example embodiment, the group controlling the content of the Web page additionally controls product availability by selecting the items that are available for purchase by children.

Yet another example of parental control is based on a password scheme. In this embodiment, the service provider requires a password from the child before allowing the child to enter the shopping area. Based on that password and input the service provider has received from the parents, the products available to the child for purchase are filtered. Thus, the parents have control over what items are made available to their children by creating a shopping profile. Such a profile could be generated, for example, as part of the application process for the Kid Card.

ISP Guide

In a preferred embodiment, the Internet Service Provider ("ISP") acts as the guide to the children's shopping experience. For example, the ISP could be America On Line ("AOL") or any other provider. Alternatively, the entity providing the Kid Card service could be a web page and not an ISP at all. However, for simplicity in the example, AOL will be used as both the ISP and the entity providing the Kid Card service.

In this example, AOL is the ISP. Additionally, AOL hosts a special "kids only" shopping area. The kids only shopping area may be accessible only with an additional password. The additional password could be assigned, for example, as part of the application process for the Kid Card. Because the kids only shopping area is within AOL, AOL is able to create the flow of the pages available to the children as they shop. Therefore, in this example, AOL guides the shopping children through the online store, displaying whatever advertisements and marketing materials deemed appropriate by AOL.

Credit/Debit Cards

In one embodiment, the Kid Card can be a credit card with a predetermined limit. Alternatively, the Kid Card can be a debit card with an available balance that has been paid in advance. For example, the application process for the debit Kid Card might require that a certain amount of money be prepaid on the debit Kid Card to cover any future purchases made with the card. In this example, when the funds are used up, the debit Kid Card no longer allows the purchase of goods. Additional funds must be paid to replenish the purchasing power of the Kid Card and allow the child to purchase additional goods.

Alternatively, in the credit card embodiment, the Kid Card can purchase items up to a certain monetary limit. For example, if the credit limit was $200.00 then purchases equaling that amount can be made before payment is required. Additionally in this example, bills must be sent out by the company providing the Kid Card shopping service.

Prepaid Gift Cards

A feature of one embodiment is the availability of prepaid gift cards. These cards operate on the same principle as a debit card or a prepaid phone card. For example, a parent could purchase a Kid Card for $200.00 and give it as a gift to a child. The child is then able to purchase $200.00 worth of goods with the Kid Card. The difference in this example embodiment is that when the funds are exhausted on the gift Kid Card, the level of funds cannot be replenished.

Disguised Mailing Feature

As stated, it is often desirable to protect the identity of consumers when ordering merchandise over the telephone, Internet or by any other means, when said merchandise is to be shipped to the residence or business of the consumer. The present invention provides a means for a consumer to order merchandise without revealing their true address to the merchant and/or shipper.

Figure 14 is a schematic diagram that depicts one embodiment of the disguised mailing feature in accordance with one embodiment of the present invention. As shown a cardholder 200 having an alias account, as described above, makes a purchase from a merchant 202. The purchase can be over the telephone, over the Internet or any other computer network, or via any other means available. The merchant uses the alias address associated with the alias account, as described above, to ship the package. In one embodiment, this alias address is a warehouse or the like, referred to herein as the disguised mailing center (DMC). Typically, a bin number associated with the Alias account is used to store the package in a specific location within the DMC. For example the Alias box number shown in the Mail Redirection data table 182, above, can be used for this purpose. The Alias box number is then used to generate a subscriber information request to the offline database to retrieve the true mailing address of the consumer.

Once this address is obtained, the package is re-labeled with the true address and sent to the consumer 208. Preferably, this takes place within twenty-four hours to avoid any further delays to the consumer.

In case of returns, the consumer is provided with a mailing label that sends the package directly back to the merchant 202. Preferably, the return address printed on the return label will be that of the DMC 204.

Alternatively, in a preferred embodiment, the re-labeling process takes place by the shipper in transit. For example, the shipper can contact a server 22, which contacts the offline database with a request for address information. The shipper can then re-label the package with the true address while the package is in transit, and thereby eliminate any extra delays.

Figure 15 is a flow chart that depicts a process that can be used to re-label packages in accordance with one embodiment of the present invention as described above. First, as shown by step 250, the consumer orders a product using an anonymous transaction technique in accordance with the present invention as described above. Accordingly, the user typically, uses an credit or debit card associated with an Alias account to purchase the merchandise.

Next as indicated by step 252, the merchant mails the package (or directs a shipper to mail the package), to the Alias address. In one embodiment, the Alias address is a warehouse or a location referred to as a disguised mailing center (DMC). Next, as indicated by step 256, the bin number (or set of characters) is input into a re-labeling system. In one example embodiment, the bin number is a unique set of characters which is used to correlate an anonymous name/address (i.e. pseudonym) with a real name/address. The bin is read into the system by scanning in a bar code or the like that comprises the bin. Alternatively, this information can be hand-keyed into the system. In any case, this action generates a request to a server that in turn contacts the bunker for the true address of the consumer. Once this information is retrieved, the package is re-labeled with the true address, as indicated by step 258. Finally, as indicated by step 260, the package is shipped to the consumer in accordance with consumer preferences (i.e. overnight, no signature necessary, etc.).

A second example of a method that can be used to re-label packages is depicted by the process flowchart in Figure 16. As indicated by step 264, the consumer orders a product from a merchant using an anonymous transaction technique as described above. As described above, package is shipped using the Alias address associated with the account. Next, as indicated by step 268, the shipper issues a request to the bunker for the true address of the consumer. This is accomplished in a manner as described above, typically through a server 23. Again, the Alias address or bin number in this example, is used to identify the consumer.

Next, as indicated by step 270, the shipper receives the true address of the consumer and re-labels the package with that address, as shown by step 272. Finally, as indicated by step 274, the package is shipped to the consumer in accordance with consumer preferences (i.e. overnight, no signature necessary, etc.).

In a third embodiment, the anonymous mailing is accomplished by mailing the merchandise to post office box, which is rented by the credit card processing company, on behalf of the cardholder. The address associated with the cardholder alias name is the post office box assigned to the cardholder. In one embodiment, the post office box is as close geographically, to the actual address of the cardholder. In this example embodiment, the cardholder picks up the merchandise from the post office box in person.

Privacy concerns also arise in connection with shipments and mail delivery unrelated to a purchase. For example, a person may wish to enter sweepstakes and order catalogs and samples without revealing own identity. Although these "transactions" do not involve payments, personal information is obtained by the provider of the information or service (also a "merchant" hereinafter). Thus, the shipment methods and systems described above are also useful for private anonymous mail delivery service. Moreover, in our increasingly mobile society, mail and packages are often lost when a person moves to a new address. Although change of address forms may be filed with the United States Postal Service, they stay in effect for only a limited period of time; public entities are also notoriously unreliable. Private mail delivery service nicely solves these problems as well, by providing a relatively more stable mailing "address" coupled with reliance on a for-profit, competitive entity having a self-interest in customer service.

One embodiment of such generic private mail service is depicted in Figure 17. Initially, the consumer (301) registers with the private mail service ("PMS" 310), which can be conceptually divided into Private Mail Administration Service ("PMAS" 311) and Private Mail Mapping Center ("PMMC" 312). PMAC is responsible for customer registration and subscription, billing, assignment of Private Mail codes, and customer service functions such as changes to delivery address, modifying account data, canceling subscriptions, as well as various other account maintenance functions.

The PMAC is accessible to customers via the Internet, telephone, and mail, although any one contact method is sufficient. Full service is preferably available through each method of customer contact.

During the registration process, see Figure 18, the PMAC obtains customer name, billing information, mail delivery address, and possibly other information. Once these data are collected and processed, the PMAC assigns a unique Private Mail Code to a customer. The code is generated by automated Private Mail Code generation process, which assigns a unique character string to be used as the Private Mail code. Next, PMAC maps the code to the customer delivery address on record. More than one code may be generated for one customer.

In order to modify any subscription data – e.g., name or address – the customer will need to authenticate his identity. The authentication process may use a personal identification number (PIN), password, digital certificate, written signature, or other means of positive identification. Customer service is preferably available for PMAC activities, so that account changes and customer issues may be resolved quickly.

After a customer's registration or other relevant transaction is processed by the PMAC, the delivery address and associated Private Mailing code is added to the PMMC and stored in its database (313). If PMAC and PMMC are physically separate from each other, a secure communication link (314) should be established between them for information transfer. All updates to the PMMC database are preferable made in real or quasi-real time. A "live" data back-up in another physical location (not pictured) is preferably maintained, so that the data is redundantly stored and service need not be interrupted if PMMC fail or PMAC fail.

Generally, consumers will not be able to update the PMMC database directly, but will have to identify themselves and follow the registration and information updating protocol established by the PMAC, as previously described. The specific update functions that consumers will be able to perform include, but are not limited to creation of a new Private Mail code, deletion of an unwanted Private Mail code, and changes to the delivery address associated with a Private Mail code.

PMMC's main function is to provide shippers with the delivery address information associated with the Private Mail code. It includes a secure interface to allow the shippers to look up the delivery address associated with a Private Mail code. Additionally, the PMMC might handle administration functions associated with the shippers, such as access control to the PMMC, usage, and billing or payment of any transaction fees or service charges.

The PMMC is preferably a high-availability service designed for continuous 24/7 operations. This will be achieved through the use of redundant equipment, multiple physical data center locations, robust disaster recovery techniques, and other means designed to prevent service interruptions. PMMC's database is highly secure, accessible only to authorized users. At a minimum, it maintains the following data: Private Mail code, physical delivery address, authorized users, and audit trail with date/time/user associated with each access.

Shippers' access to the PMMC database is restricted to look-up operations that map a Private Mail code to a delivery address, and to access to certain administrative functions of the PMCC that are used for troubleshooting, problem resolution, and account maintenance.

After a customer's registration is completed, the Private Mail Service is activated. Following activation, the customer has a brand-new address -- the Private Mailing code assigned.

Figure 19 shows a flowchart of a typical transaction, which, of course, need not be a purchase, but instead may be any interaction that results in a mailing or shipping. The customer provides the Private Mail code to a merchant to enable the merchant to ship mail or parcels to the customer. Using the example of an online purchase, the customer orders from the merchant in the usual way, but supplies only the Private Mail code as the "ship to" address. The merchant then fills the order and labels it for shipment using only the Private Mail code. The parcel is picked up by the shipper. The shipper, a Private Mail partner, accesses the PMMC to map the Private Mail code on the parcel to the customer's physical delivery address. Once the mapping is completed, the shipper re-labels the parcel, either physically or electronically, with the delivery address and completes the delivery using conventional means.

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for protecting anonymity of a consumer when ordering merchandise to be delivered to the consumer, the method comprising the steps of:

ordering merchandise using an alias credit or debit card, wherein the alias credit or debit card has an associated pseudonym and an associated true name and address of the consumer;

shipping the merchandise using the pseudonym, wherein the pseudonym includes an address associated with a disguised mailing center (DMC);

communicating the pseudonym to an offline database comprising the true name and address associated with the pseudonym;

retrieving the true address;

re-labeling the merchandise with the true address; and

shipping the merchandise from the DMC to the true address.

2. The method of claim 1, wherein the pseudonym comprises an alias address.

3. The method of claim 1, wherein the pseudonym further comprises an alias name.

4. The method of claim 1, further comprising the step of re-labeling the merchandise with the true name.

5. The method of claim 1, wherein said communicating step comprises the steps of:

generating a request for subscriber information to a central server;

processing the request at the central server;

sending the request from the central server to the offline database;

receiving a response from the offline database at the server; and

sending the response from the server to the DMC.

6. The method of claim 1, wherein the pseudonym includes a bin number.

7. The method of claim 6, wherein the bin number is used as a destination within the DMC.

8. The method of claim 1, wherein the pseudonym is automatically scanned into a re-labeling system.

9. A method for protecting anonymity of a consumer when ordering merchandise to be delivered to the consumer, the method comprising the steps of:

ordering merchandise using an alias credit or debit card, wherein the alias credit or debit card has an associated alias name/address and an associated true address of the consumer;

shipping the merchandise using the alias name/address;

communicating the alias name/address to an offline database comprising the true address and the alias address;

retrieving the true name/address; and

re-labeling the merchandise with the true name/address.

10. The method of claim 9, wherein the communicating, retrieving, and re-labeling steps are accomplished by the shipper while the merchandise is in transit.

11. The method of claim 10, wherein the communicating step is accomplished by the shipper using a wireless connection to a central server.

12. The method of claim 9, wherein said communicating step comprises the steps of:

generating a request for subscriber information to a central server while the merchandise is in transit by the shipper;

processing the request at the central server;

sending the request from the central server to the offline database;

receiving a response from the offline database at the server; and

sending the response from the server to the shipper.

13. The method of claim 9, wherein the alias address includes a bin number.

14. The method of claim 9, wherein the alias name/address is automatically scanned into a re-labeling system.

15. A system for protecting anonymity of a consumer when ordering merchandise to be delivered to the consumer, the system comprising:

means for ordering merchandise using an alias credit or debit card, wherein the alias credit or debit card has an associated alias name/address and an associated true name/address of the consumer;

means for shipping the merchandise using the alias name/address, wherein the alias name/address is a disguised mailing center (DMC);

means for communicating the alias name/address to an offline database comprising the true name/address and the alias name/address;

means for retrieving the true name/address;

means for re-labeling the merchandise with the true name/address; and

means for shipping the merchandise from the DMC to the true name/address.

16. The system of claim 15, wherein said means for communicating comprises:

means for generating a request for subscriber information to a central server;

means for processing the request at the central server;

means for sending the request from the central server to the offline database;

receiving a response from the offline database at the server; and

sending the response from the server to the DMC.

17. The system of claim 15, wherein the alias name/address includes a bin number.

18. The system of claim 17, wherein the bin number is used as a destination within the DMC.

19. The system of claim 15, wherein the alias name/address is automatically scanned into a re-labeling system.

20. A system for protecting anonymity of a consumer when ordering merchandise to be delivered to the consumer comprising:

means for ordering merchandise using an alias credit or debit card, wherein the alias credit or debit card has an associated alias name/address and an associated true name/address of the consumer;

means for shipping the merchandise using the alias name/address;

means for communicating the alias name/address to an offline database comprising the true name/address and the alias name/address;

means for retrieving the true name/address; and

means for re-labeling the merchandise with the true name/address.

21. The system of claim 20, wherein the means for communicating, retrieving, and re-labeling are performed by the shipper while the merchandise is in transit.

22. The system of claim 20, wherein the means for communicating includes a wireless connection from the shipper to a central server.

23. The system of claim 21, wherein the means for communicating comprises:

means for generating a request for subscriber information to a central server while the merchandise is in transit by the shipper;

means for processing the request at the central server;

means for sending the request from the central server to the offline database;

means for receiving a response from the offline database at the server; and

means for sending the response from the server to the shipper.

24. An anonymous mailing method for shipping an item from an item provider to a customer having a first physical delivery address, by a shipper, without disclosing to the item provider the first physical delivery address, the method comprising the following steps:

mapping a first unique personal mail code to the first delivery address;

receiving from the shipper a request to resolve the first code into a physical delivery address;

resolving the first code into the first delivery address; and

returning to the shipper the first delivery address, thereby enabling the shipper to deliver the item to the customer at the location associated with the first physical delivery address.

25. The method of claim 24, further comprising the steps of:

registering the customer with a private mail service;

generating the first unique personal mail code;

assigning the first unique personal mail code to the customer after the step of registering the customer.

26. The method according to claim 25, further comprising the step of providing a secure communication channel for receiving from the shipper the request to resolve and returning to the shipper the first delivery address.

27. The method of claim 26, further comprising the step of ordering the item from the item provider for delivery at the location associated with the first delivery address.

28. The method of claim 27, further comprising the steps of:

requesting the item by the customer from the item provider;

disclosing to the item provider the first code by the customer;

labeling the item with the first code; and

giving the item to the shipper for shipment in accordance with the label.

29. The method of claim 27, wherein the code, the first delivery address, and the mapping from the first code to the first delivery address are stored at an offline database.

30. The method of claim 29, further comprising the step of retrieving the first delivery address from the offline database, the step of retrieving the first delivery address

being performed after the step of resolving the code, the step of retrieving the first delivery address being performed before the step of returning to the shipper the first delivery address.

31. The method of claim 26, further comprising the steps of:

re-labeling the item physically or electronically with the first delivery address; and

delivering the item to the physical location associated with the first physical address.

32. The method of claim 26, wherein the steps of mapping, resolving, receiving from the shipper a request, returning to the shipper the first delivery address, registering the customer, and generating the first code are performed by the private mail service.

33. The method of claim 25, wherein the step of registering the customer includes the steps of:

providing to the private mail service the customer's name and the first delivery address;

paying the private mail service;

creating a secret customer identifier;

sending the secret customer identifier to the customer; and

confirming receipt of the secret customer identifier by the customer,

thereby enabling the customer positively to identify the customer to the private mail service by submitting the secret customer identifier.

34. The method of claim 33, further comprising the steps of:

receiving from the customer a request to change the customer's mail code;

after receiving from the customer the request to change, requesting the customer to positively identify the customer;

after the customer is identified, generating a second unique personal mail code, assigning the second unique personal mail code to the customer, mapping the second unique personal mail code to the first physical delivery address, and deleting the mapping of the first unique personal mail code to the first physical delivery address.

35. The method of claim 26, further comprising the step of registering the shipper with the private mail service, the step of registering the shipper including the steps of providing the shipper with means for accessing the secure communication channel.

36. An anonymous mailing method for shipping an item from an item provider to a customer, by a shipper, without disclosing to the item provider the customer's physical delivery address, the method comprising the following steps:

registering the customer with a private mail service, including the steps of:

receiving by the private mail service the customer's name and the customer's first physical delivery address,

receiving customer payment by the private mail service,

selecting a secret customer identifier,

sending the secret customer identifier to the customer,

confirming receipt of the secret customer identifier by the customer,

thereby enabling the customer positively to identify the customer to the private mail service by submitting the secret customer identifier;

storing the customer's name, the customer's first physical delivery address, and the secret customer identifier in a database;

generating a first unique personal mail code;

assigning the first unique personal mail code to the customer;

mapping the first unique personal mail code to the customer's first physical delivery address;

receiving from the customer a request to update the customer's physical delivery address;

after receiving from the customer the request to update, requesting the customer to positively identify the customer;

after the customer is identified, receiving from the customer the customer's second physical delivery address;

storing the customer's second delivery address in the database;

asking the customer whether the customer requires a new personal mail code;

if the customer requires a new personal mail code, generating a second unique personal mail code, assigning the second unique personal mail code to the customer, and mapping the second unique personal mail code to the customer's second physical delivery address;

receiving from the shipper a request to resolve the second personal mail code into a physical delivery address;

resolving the second personal mail code into the customer's second physical delivery address; and

returning to the shipper the customer's second physical delivery address,

thereby enabling the shipper to deliver the item to the customer at the location associated with the customer's second physical delivery address.

37. A private mail system for shipping an item from an item provider to a customer at a physical delivery address, by a shipper, without disclosing to the item provider the customer's physical delivery address, the system comprising:

a customer registration facility;

a facility mapping a mail code to the customer's physical delivery address;

a communication mechanism for communicating with a shipper, the mechanism for communicating with the shipper including a mechanism for receiving from the shipper a request to resolve the mail code into a physical delivery address and a mechanism for returning to the shipper the customer's physical delivery address;

mechanism for resolving the mail code into the customer's physical delivery address,

whereby communicating the customer's physical delivery address to the shipper enables the shipper to deliver an item labeled with the mail code to the customer's physical delivery address.

38. The system of claim 37, further comprising:

a mail code generator;

a mechanism for assigning the mail code to the customer; and

a database for storing the customer's name, the customer's physical delivery address, the mail code, and the mapping between the mail code and the customer's physical delivery address.

39. The system of claim 38, further comprising:

an identifier for positively identifying the customer; and

a shipper registration facility;

wherein:

the means for returning to the shipper the customer's physical delivery address is inoperative until the shipper registers with the system; and the means for communicating is a secure encrypted electronic means for communicating.

40. A method for using the system of claim 37 to deliver the item, the method comprising the steps of:

registering with the system;

receiving from the shipper the item labeled with the mail code;

requesting the system to resolve the mail code into a physical delivery address;

receiving from the system the customer's physical delivery address; and

delivering the item to the location associated with the customer's physical delivery address.

41. A method for using the system of claim 37 to ship the item to the customer without knowing the customer's physical deliveryn address, the method comprising the steps of:

receiving from the customer the mail code;

labeling the item with the mail code;

delivering the item to the shipper after the shipper registers with the system; and

instructing the shipper to deliver the package to the customer.

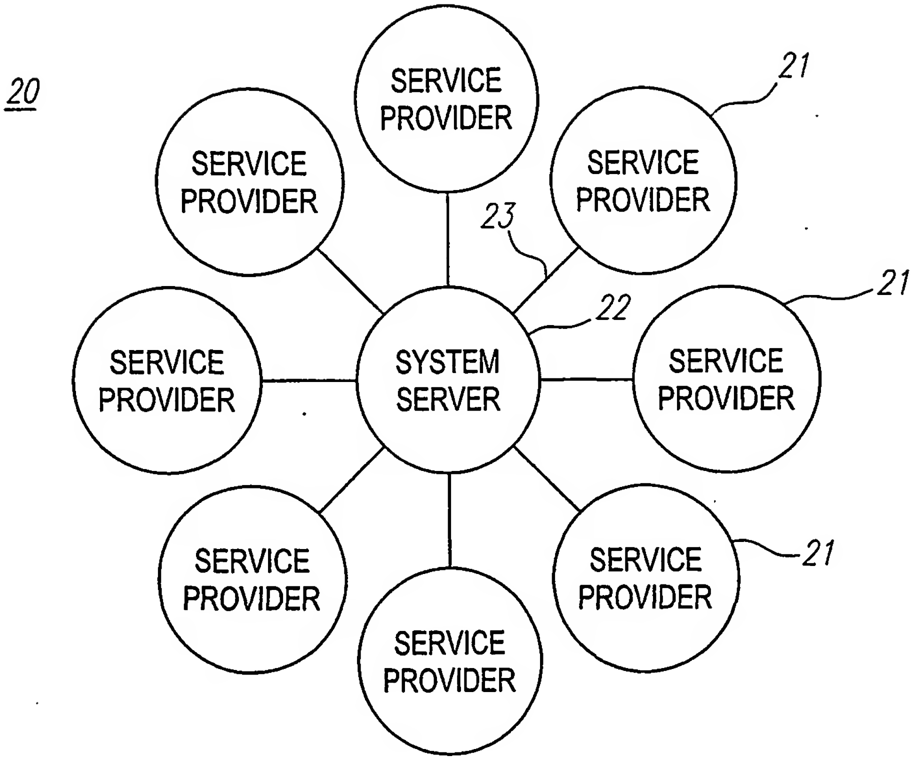

20
SERVICE PROVIDER
SERVICE PROVIDER
SERVICE PROVIDER
21
23
SERVICE PROVIDER
SYSTEM SERVER
22
SERVICE PROVIDER
21
SERVICE PROVIDER
SERVICE PROVIDER
SERVICE PROVIDER
21

FIG. 1

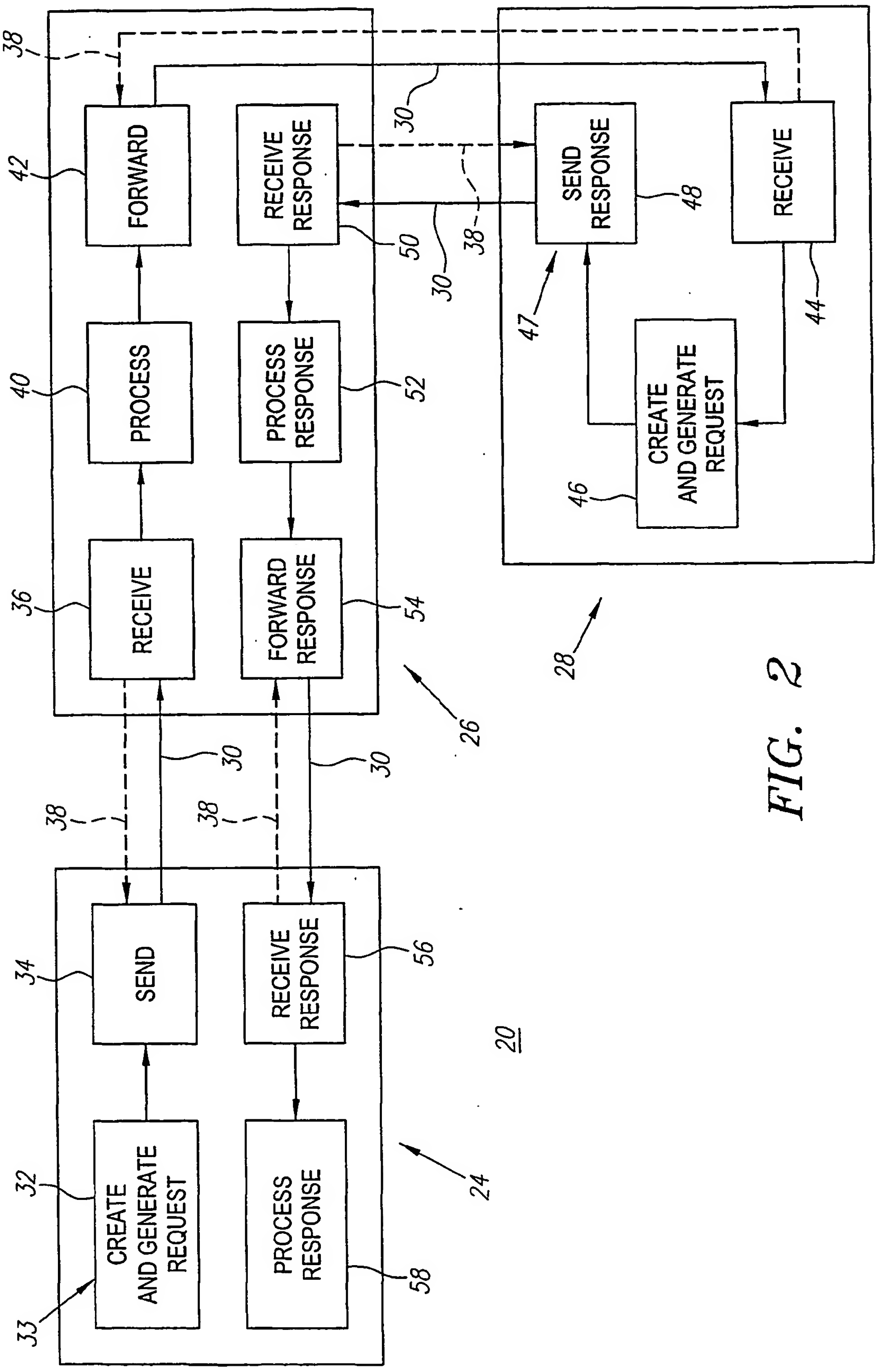

FORWARD
PROCESS
RECEIVE
RECEIVE RESPONSE
PROCESS RESPONSE
FORWARD RESPONSE
SEND RESPONSE
RECEIVE
CREATE AND GENERATE REQUEST
SEND
RECEIVE RESPONSE
CREATE AND GENERATE REQUEST
PROCESS RESPONSE
20
24
26
28
30
32
33
34
36
38
40
42
44
46
47
48
50
52
54
56
58

FIG. 2

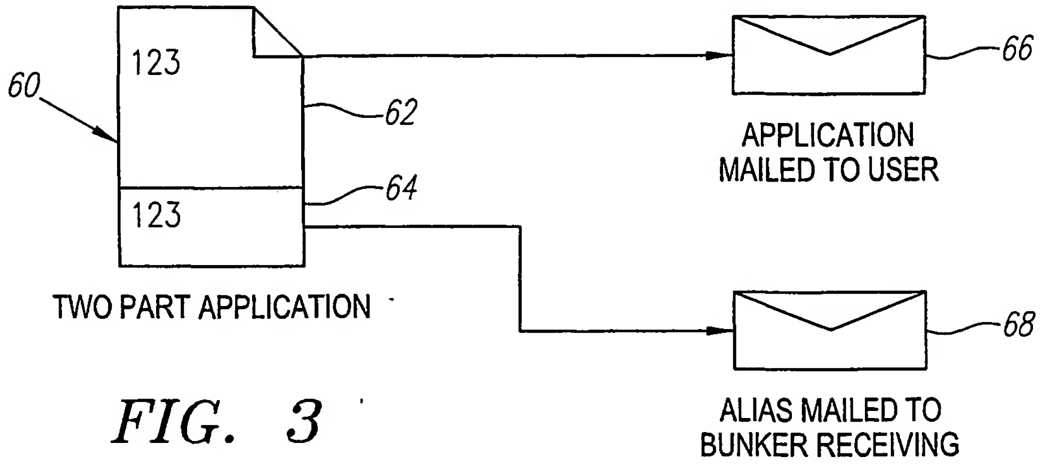

60
123
123
62
64
TWO PART APPLICATION
66
APPLICATION MAILED TO USER
68
ALIAS MAILED TO BUNKER RECEIVING

FIG. 3

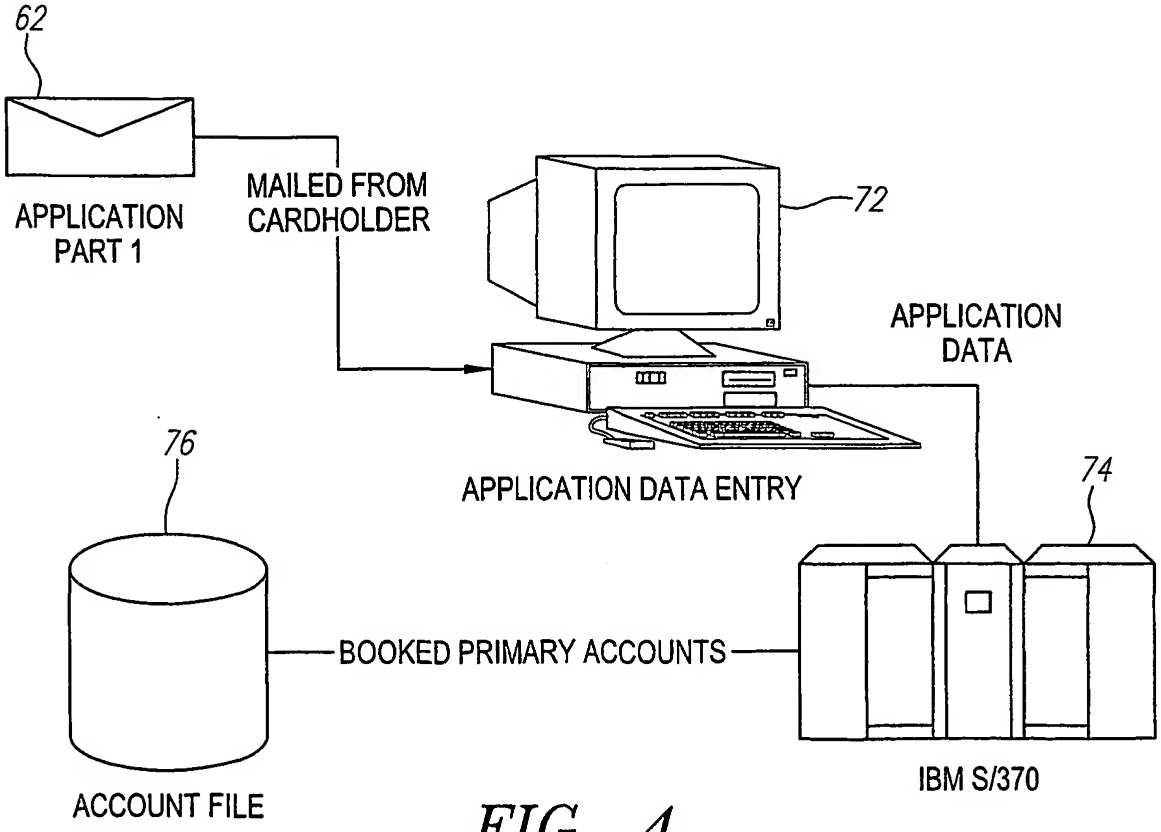

62
APPLICATION PART 1
MAILED FROM CARDHOLDER
72
APPLICATION DATA
APPLICATION DATA ENTRY
76
74
BOOKED PRIMARY ACCOUNTS
ACCOUNT FILE
IBM S/370

FIG. 4

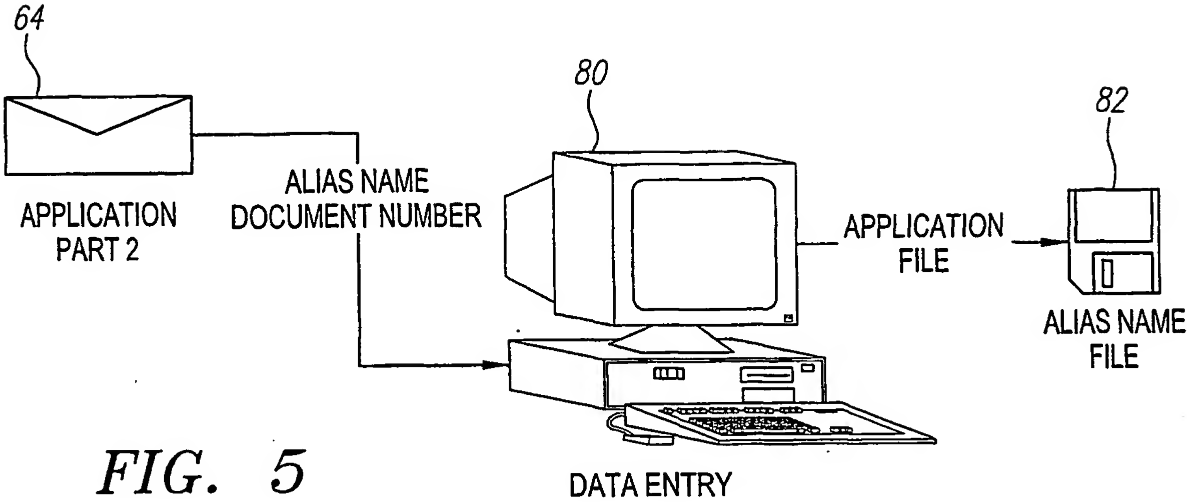

64
APPLICATION PART 2
ALIAS NAME DOCUMENT NUMBER
80
APPLICATION FILE
82
ALIAS NAME FILE
DATA ENTRY

FIG. 5

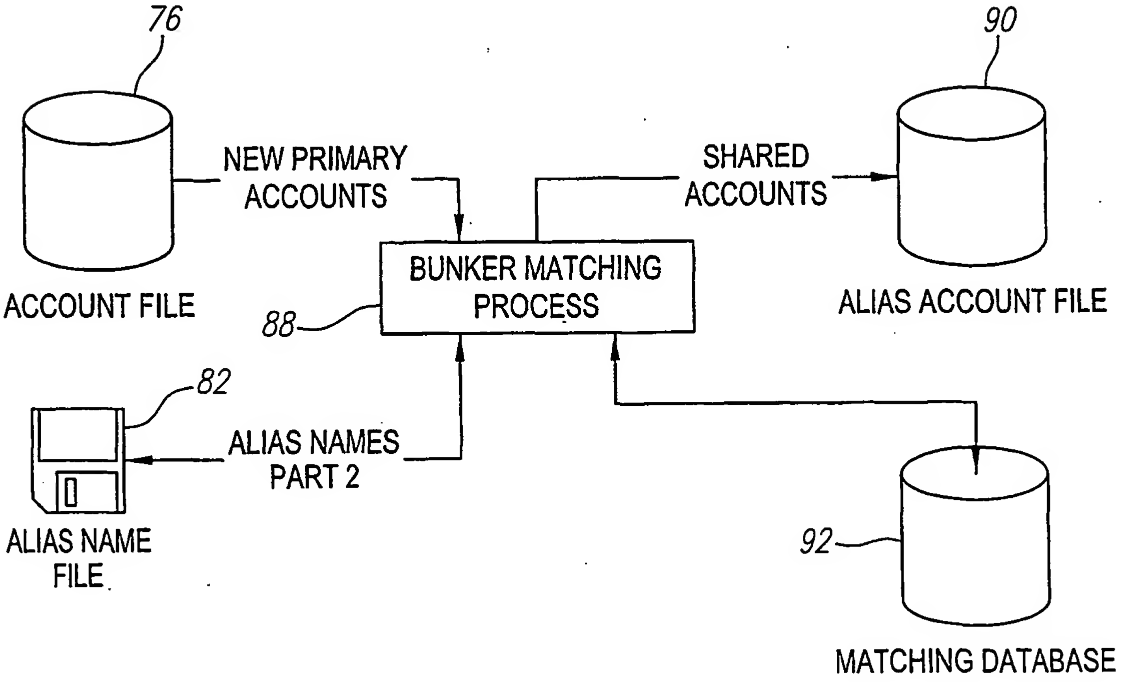

76
ACCOUNT FILE
NEW PRIMARY ACCOUNTS
BUNKER MATCHING PROCESS
88
SHARED ACCOUNTS
90
ALIAS ACCOUNT FILE
82
ALIAS NAMES PART 2
ALIAS NAME FILE
92
MATCHING DATABASE

FIG. 6A

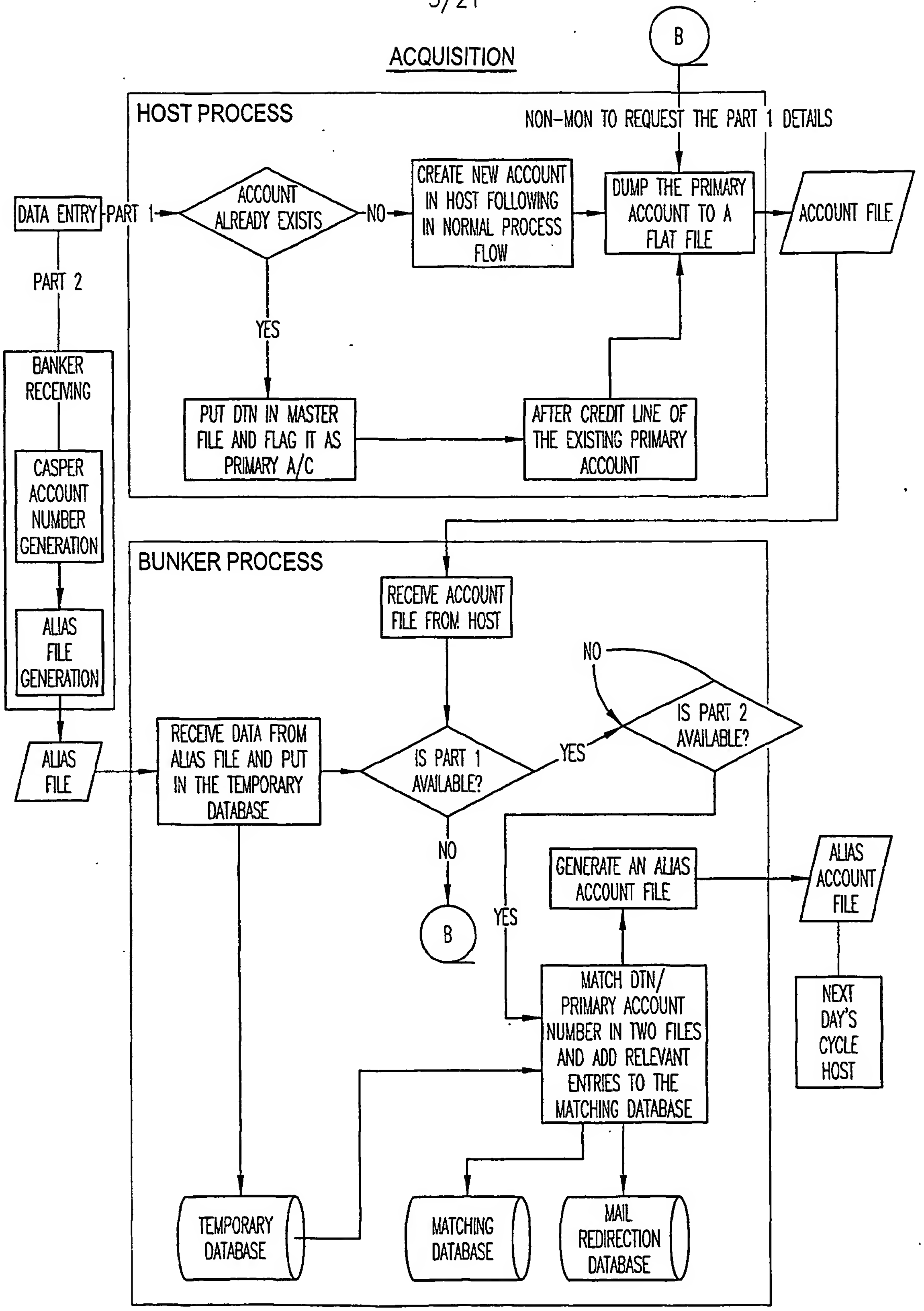

ACQUISITION
B
HOST PROCESS
NON-MON TO REQUEST THE PART 1 DETAILS
DATA ENTRY
PART 1
ACCOUNT ALREADY EXISTS
NO
CREATE NEW ACCOUNT IN HOST FOLLOWING IN NORMAL PROCESS FLOW
DUMP THE PRIMARY ACCOUNT TO A FLAT FILE
ACCOUNT FILE
PART 2
YES
BANKER RECEIVING
CASPER ACCOUNT NUMBER GENERATION
ALIAS FILE GENERATION
PUT DTN IN MASTER FILE AND FLAG IT AS PRIMARY A/C
AFTER CREDIT LINE OF THE EXISTING PRIMARY ACCOUNT
BUNKER PROCESS
RECEIVE ACCOUNT FILE FROM HOST
NO
IS PART 2 AVAILABLE?
YES
ALIAS FILE
RECEIVE DATA FROM ALIAS FILE AND PUT IN THE TEMPORARY DATABASE
IS PART 1 AVAILABLE?
NO
B
YES
GENERATE AN ALIAS ACCOUNT FILE
ALIAS ACCOUNT FILE
MATCH DTN/ PRIMARY ACCOUNT NUMBER IN TWO FILES AND ADD RELEVANT ENTRIES TO THE MATCHING DATABASE
NEXT DAY'S CYCLE HOST
TEMPORARY DATABASE
MATCHING DATABASE
MAIL REDIRECTION DATABASE

FIG. 6B

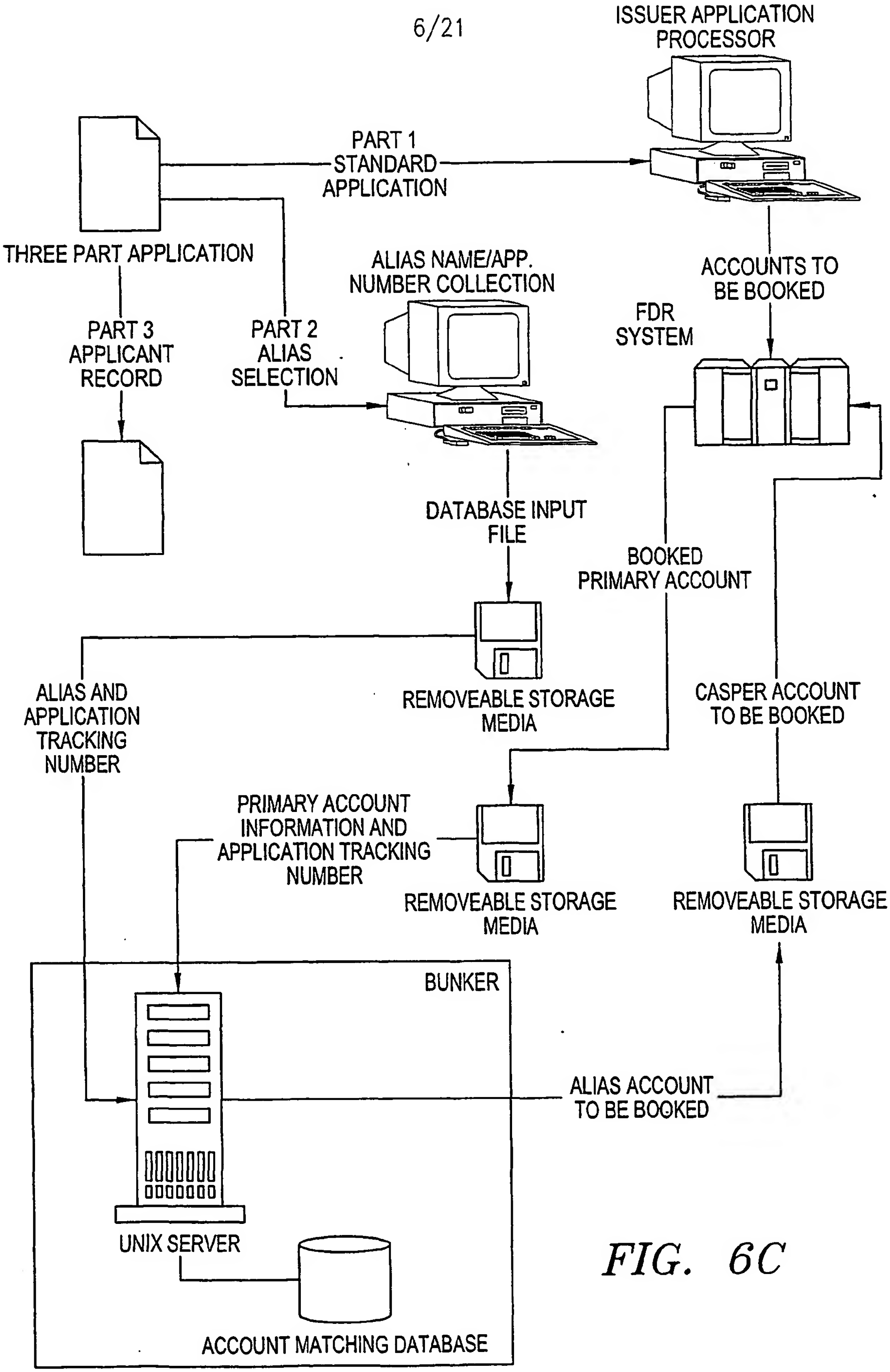

ISSUER APPLICATION PROCESSOR
PART 1 STANDARD APPLICATION
THREE PART APPLICATION
ALIAS NAME/APP. NUMBER COLLECTION
ACCOUNTS TO BE BOOKED
FDR SYSTEM
PART 3 APPLICANT RECORD
PART 2 ALIAS SELECTION
DATABASE INPUT FILE
BOOKED PRIMARY ACCOUNT
ALIAS AND APPLICATION TRACKING NUMBER
REMOVEABLE STORAGE MEDIA
CASPER ACCOUNT TO BE BOOKED
PRIMARY ACCOUNT INFORMATION AND APPLICATION TRACKING NUMBER
REMOVEABLE STORAGE MEDIA
REMOVEABLE STORAGE MEDIA
BUNKER
ALIAS ACCOUNT TO BE BOOKED
UNIX SERVER
ACCOUNT MATCHING DATABASE

FIG. 6C

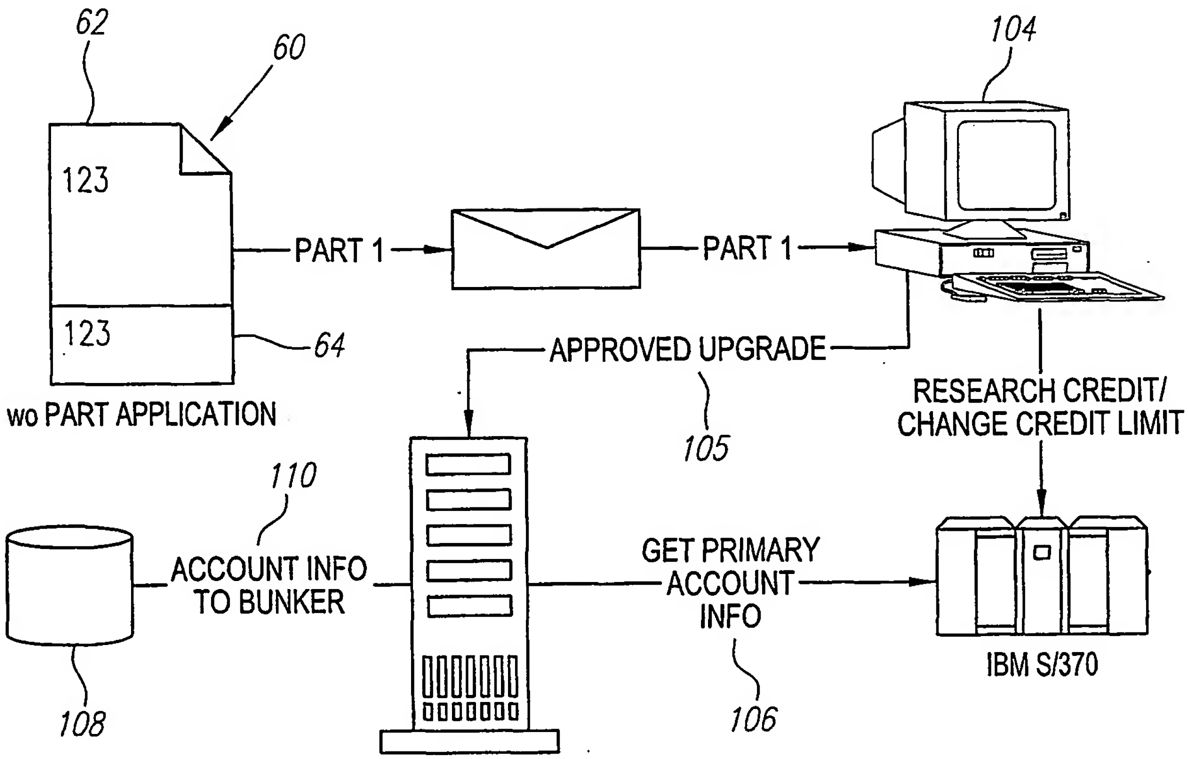

62
60
104
123
PART 1
PART 1
123
64
APPROVED UPGRADE
wo PART APPLICATION
RESEARCH CREDIT/ CHANGE CREDIT LIMIT
105
110
ACCOUNT INFO TO BUNKER
GET PRIMARY ACCOUNT INFO
IBM S/370
108
106

FIG. 7

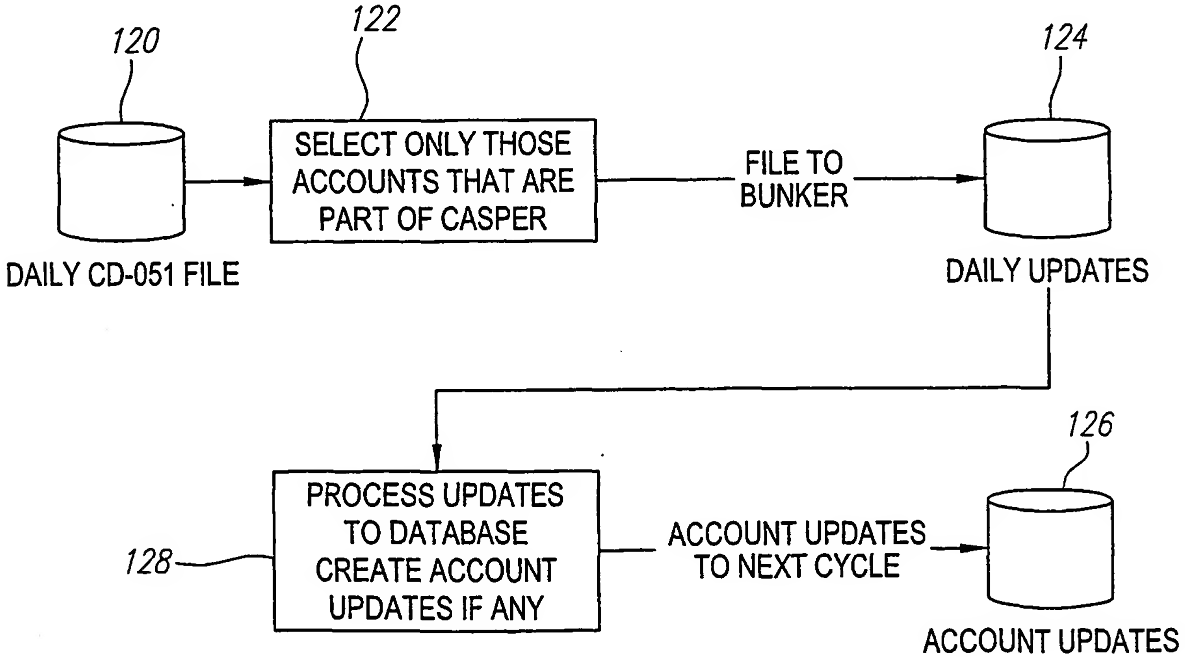

120
122
124
SELECT ONLY THOSE ACCOUNTS THAT ARE PART OF CASPER
FILE TO BUNKER
DAILY CD-051 FILE
DAILY UPDATES
126
128
PROCESS UPDATES TO DATABASE CREATE ACCOUNT UPDATES IF ANY
ACCOUNT UPDATES TO NEXT CYCLE
ACCOUNT UPDATES

FIG. 8A

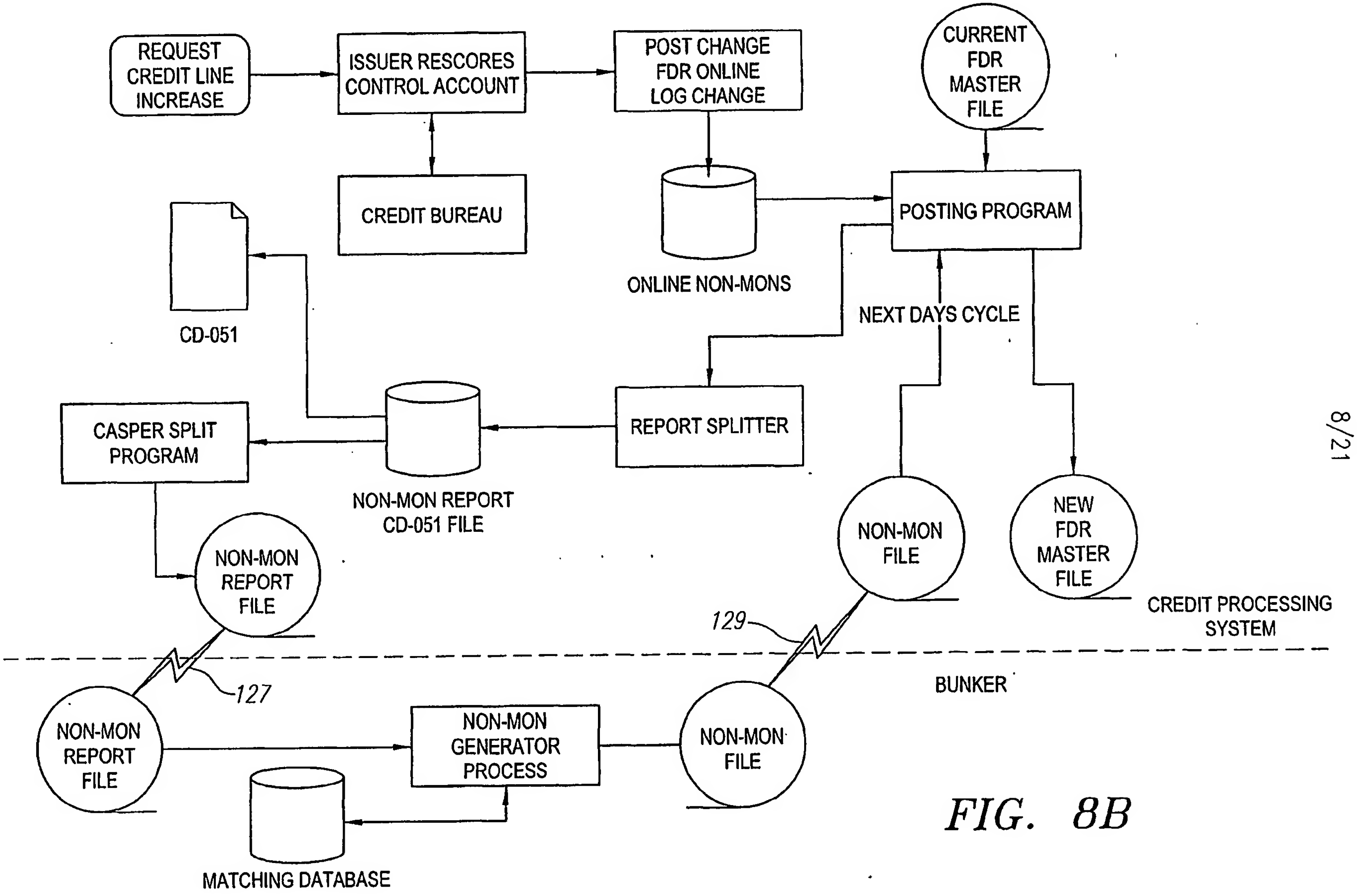
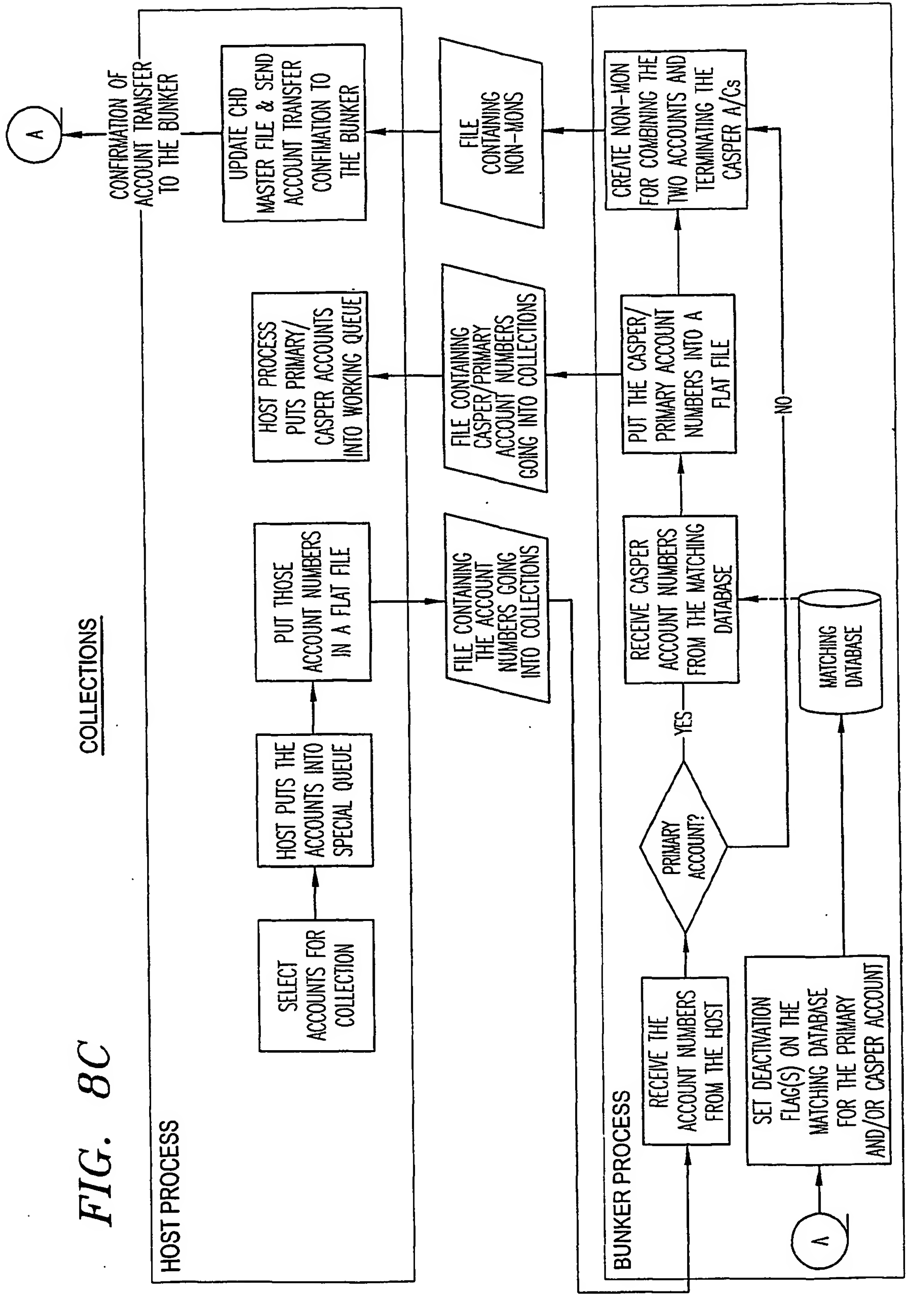

REQUEST CREDIT LINE INCREASE
ISSUER RESCORES CONTROL ACCOUNT
CREDIT BUREAU
POST CHANGE FDR ONLINE LOG CHANGE
ONLINE NON-MONS
CURRENT FDR MASTER FILE
POSTING PROGRAM
NEXT DAYS CYCLE
NEW FDR MASTER FILE
NON-MON FILE
CREDIT PROCESSING SYSTEM
REPORT SPLITTER
NON-MON REPORT CD-051 FILE
CD-051
CASPER SPLIT PROGRAM
NON-MON REPORT FILE
129
127
BUNKER
NON-MON REPORT FILE
NON-MON GENERATOR PROCESS
NON-MON FILE
MATCHING DATABASE

FIG. 8B

FIG. 8C

COLLECTIONS


HOST PROCESS
SELECT ACCOUNTS FOR COLLECTION
HOST PUTS THE ACCOUNTS INTO SPECIAL QUEUE
PUT THOSE ACCOUNT NUMBERS IN A FLAT FILE
FILE CONTAINING THE ACCOUNT NUMBERS GOING INTO COLLECTIONS
HOST PROCESS PUTS PRIMARY/ CASPER ACCOUNTS INTO WORKING QUEUE
FILE CONTAINING CASPER/PRIMARY ACCOUNT NUMBERS GOING INTO COLLECTIONS
UPDATE CHD MASTER FILE & SEND ACCOUNT TRANSFER CONFIMATION TO THE BUNKER
FILE CONTAINING NON-MONS
CONFIRMATION OF ACCOUNT TRANSFER TO THE BUNKER
A
BUNKER PROCESS
RECEIVE THE ACCOUNT NUMBERS FROM THE HOST
PRIMARY ACCOUNT?
YES
NO
RECEIVE CASPER ACCOUNT NUMBERS FROM THE MATCHING DATABASE
PUT THE CASPER/ PRIMARY ACCOUNT NUMBERS INTO A FLAT FILE
CREATE NON-MON FOR COMBINING THE TWO ACCOUNTS AND TERMINATING THE CASPER A/Cs
MATCHING DATABASE
SET DEACTIVATION FLAG(S) ON THE MATCHING DATABASE FOR THE PRIMARY AND/OR CASPER ACCOUNT
A

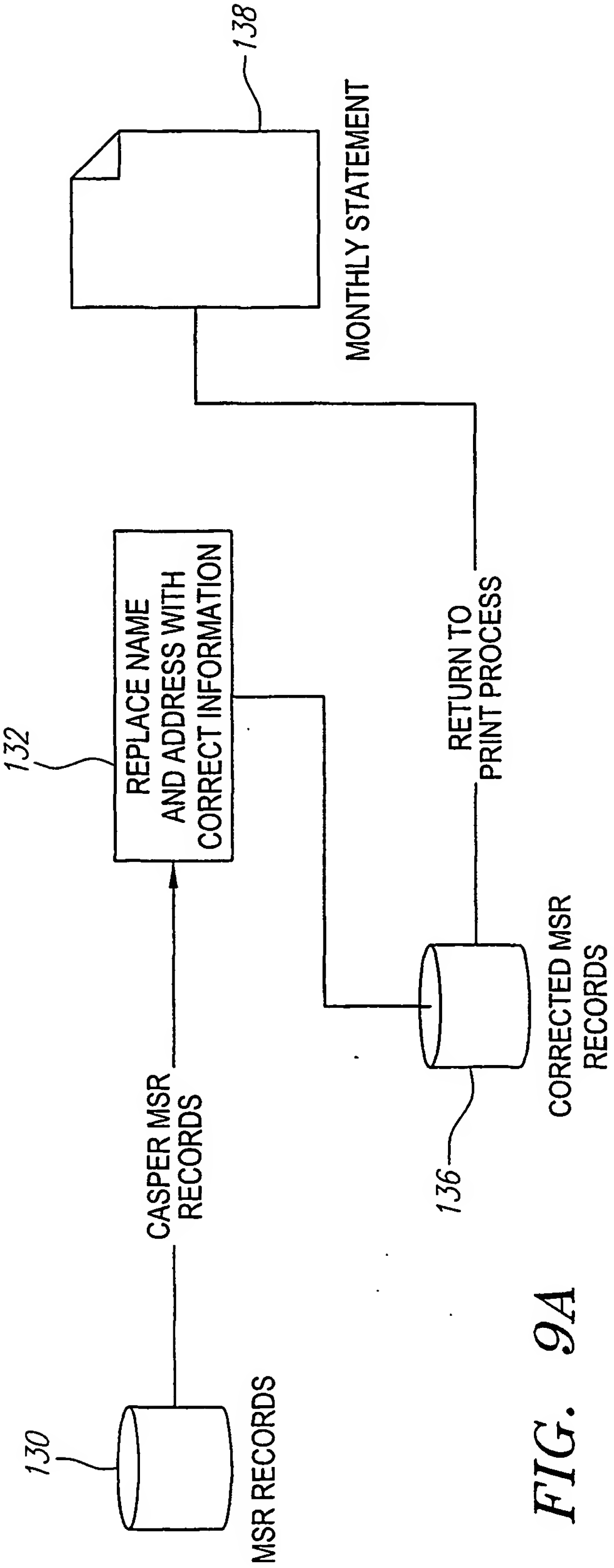

130
MSR RECORDS
CASPER MSR RECORDS
132
REPLACE NAME AND ADDRESS WITH CORRECT INFORMATION
136
CORRECTED MSR RECORDS
RETURN TO PRINT PROCESS
138
MONTHLY STATEMENT

FIG. 9A

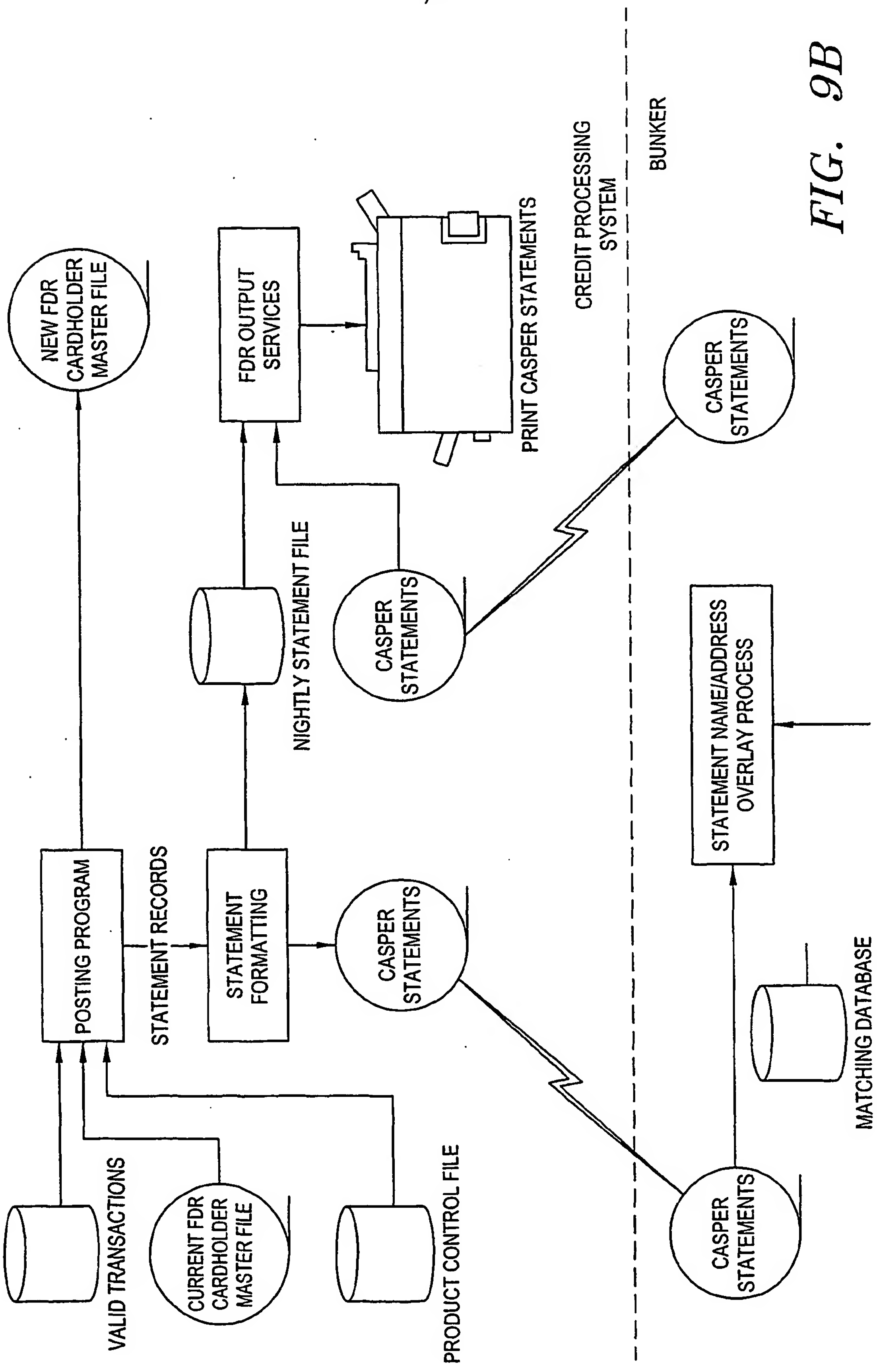

VALID TRANSACTIONS
CURRENT FDR CARDHOLDER MASTER FILE
PRODUCT CONTROL FILE
POSTING PROGRAM
NEW FDR CARDHOLDER MASTER FILE
STATEMENT RECORDS
STATEMENT FORMATTING
NIGHTLY STATEMENT FILE
FDR OUTPUT SERVICES
PRINT CASPER STATEMENTS
CASPER STATEMENTS
CASPER STATEMENTS
CREDIT PROCESSING SYSTEM
BUNKER
CASPER STATEMENTS
CASPER STATEMENTS
MATCHING DATABASE
STATEMENT NAME/ADDRESS OVERLAY PROCESS

FIG. 9B

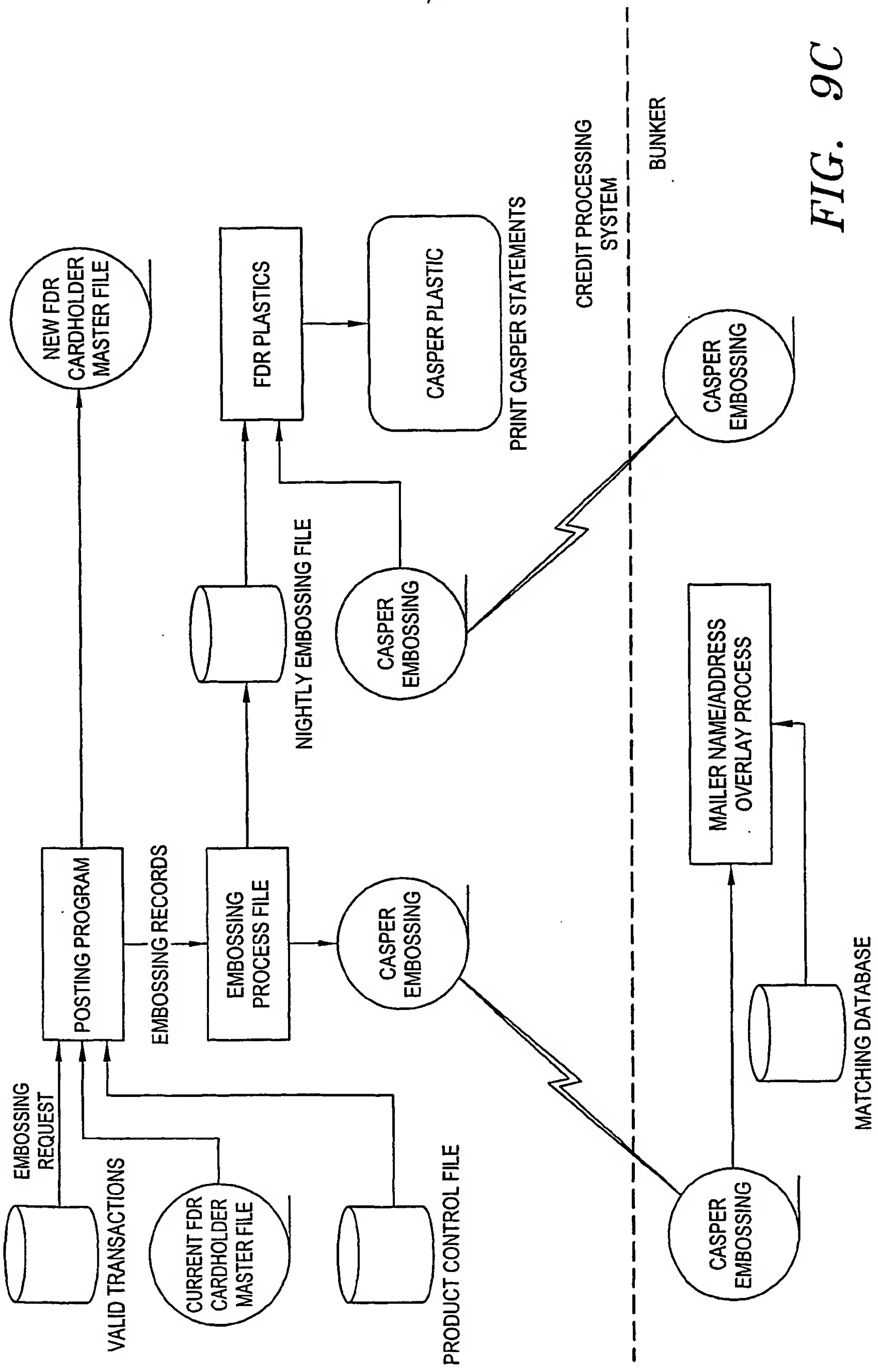

EMBOSSING REQUEST
VALID TRANSACTIONS
CURRENT FDR CARDHOLDER MASTER FILE
PRODUCT CONTROL FILE
POSTING PROGRAM
EMBOSSING RECORDS
EMBOSSING PROCESS FILE
CASPER EMBOSSING
NEW FDR CARDHOLDER MASTER FILE
NIGHTLY EMBOSSING FILE
CASPER EMBOSSING
FDR PLASTICS
CASPER PLASTIC
PRINT CASPER STATEMENTS
CREDIT PROCESSING SYSTEM
BUNKER
CASPER EMBOSSING
CASPER EMBOSSING
MAILER NAME/ADDRESS OVERLAY PROCESS
MATCHING DATABASE

FIG. 9C

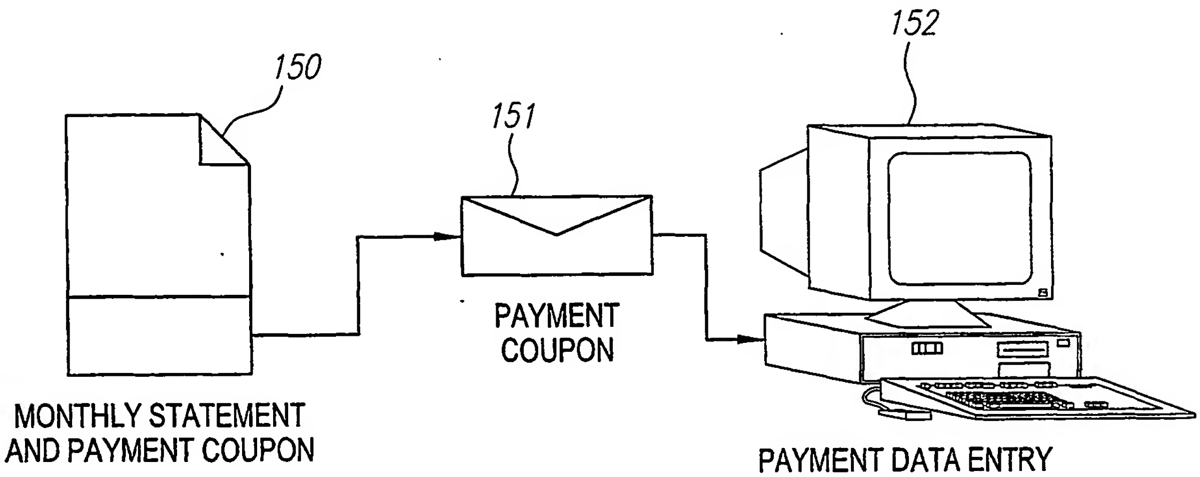


FIG. 10

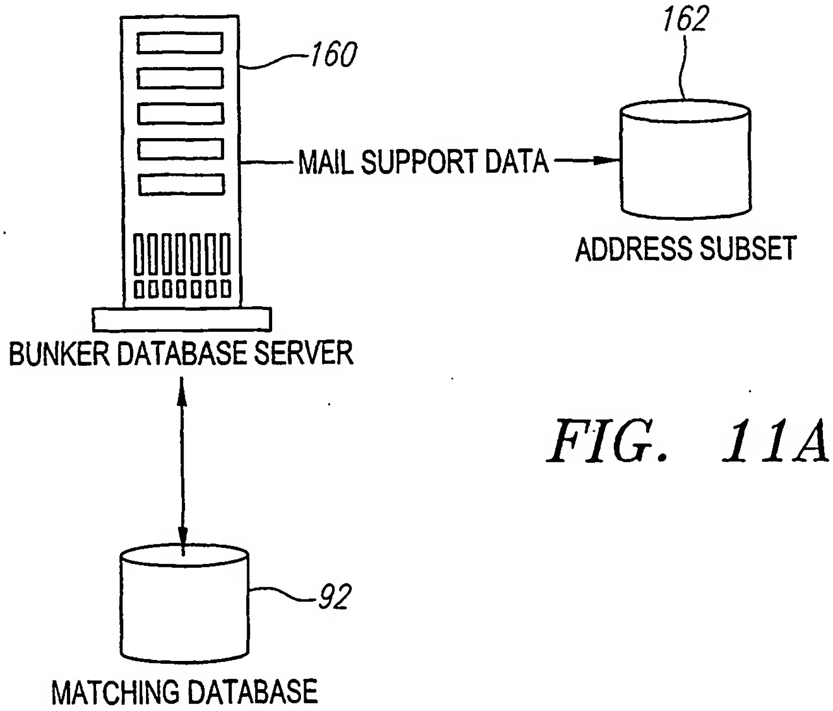


FIG. 11A

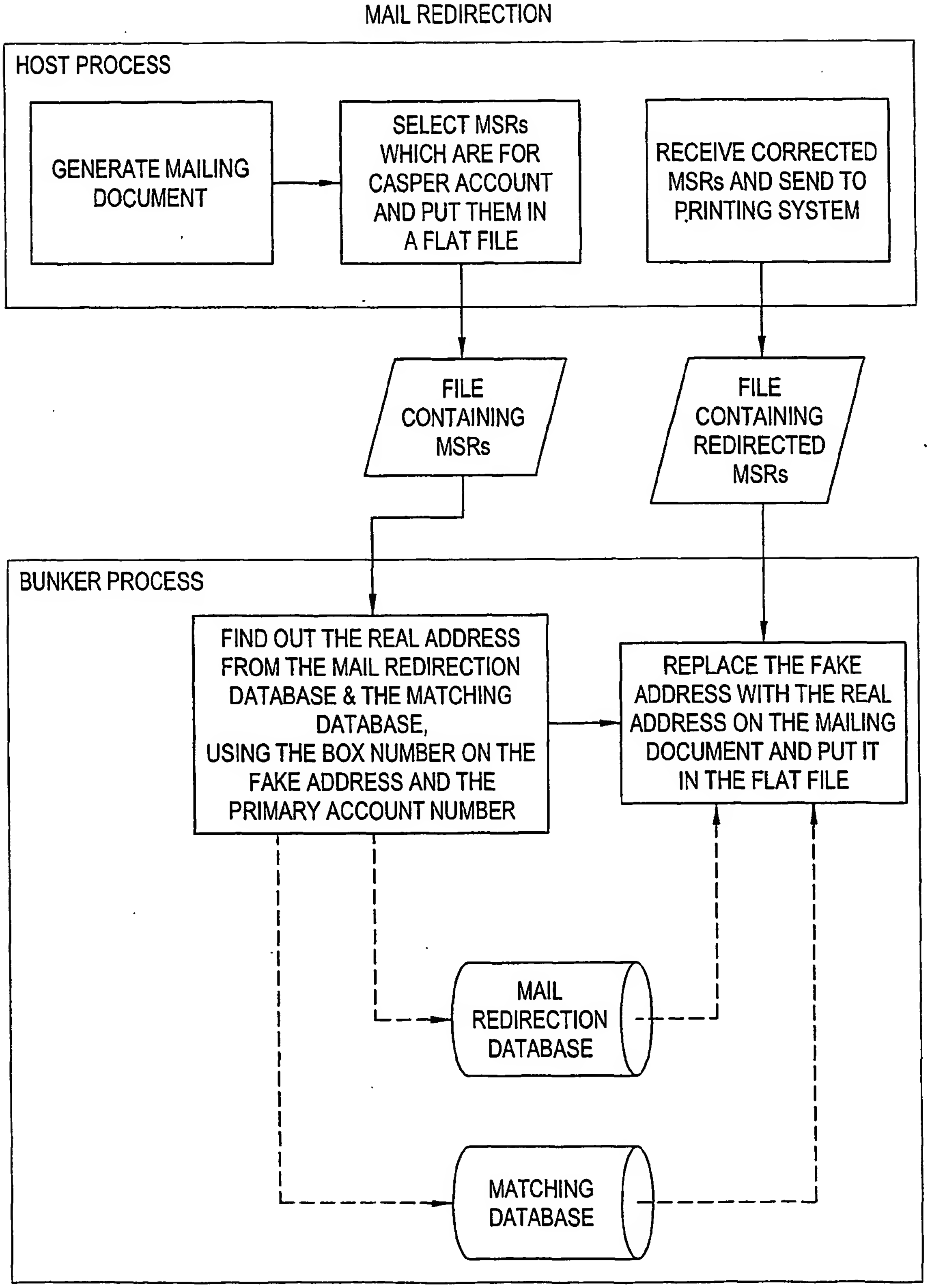

MAIL REDIRECTION
HOST PROCESS
GENERATE MAILING DOCUMENT
SELECT MSRs WHICH ARE FOR CASPER ACCOUNT AND PUT THEM IN A FLAT FILE
RECEIVE CORRECTED MSRs AND SEND TO PRINTING SYSTEM
FILE CONTAINING MSRs
FILE CONTAINING REDIRECTED MSRs
BUNKER PROCESS
FIND OUT THE REAL ADDRESS FROM THE MAIL REDIRECTION DATABASE & THE MATCHING DATABASE, USING THE BOX NUMBER ON THE FAKE ADDRESS AND THE PRIMARY ACCOUNT NUMBER
REPLACE THE FAKE ADDRESS WITH THE REAL ADDRESS ON THE MAILING DOCUMENT AND PUT IT IN THE FLAT FILE
MAIL REDIRECTION DATABASE
MATCHING DATABASE

FIG. 11B

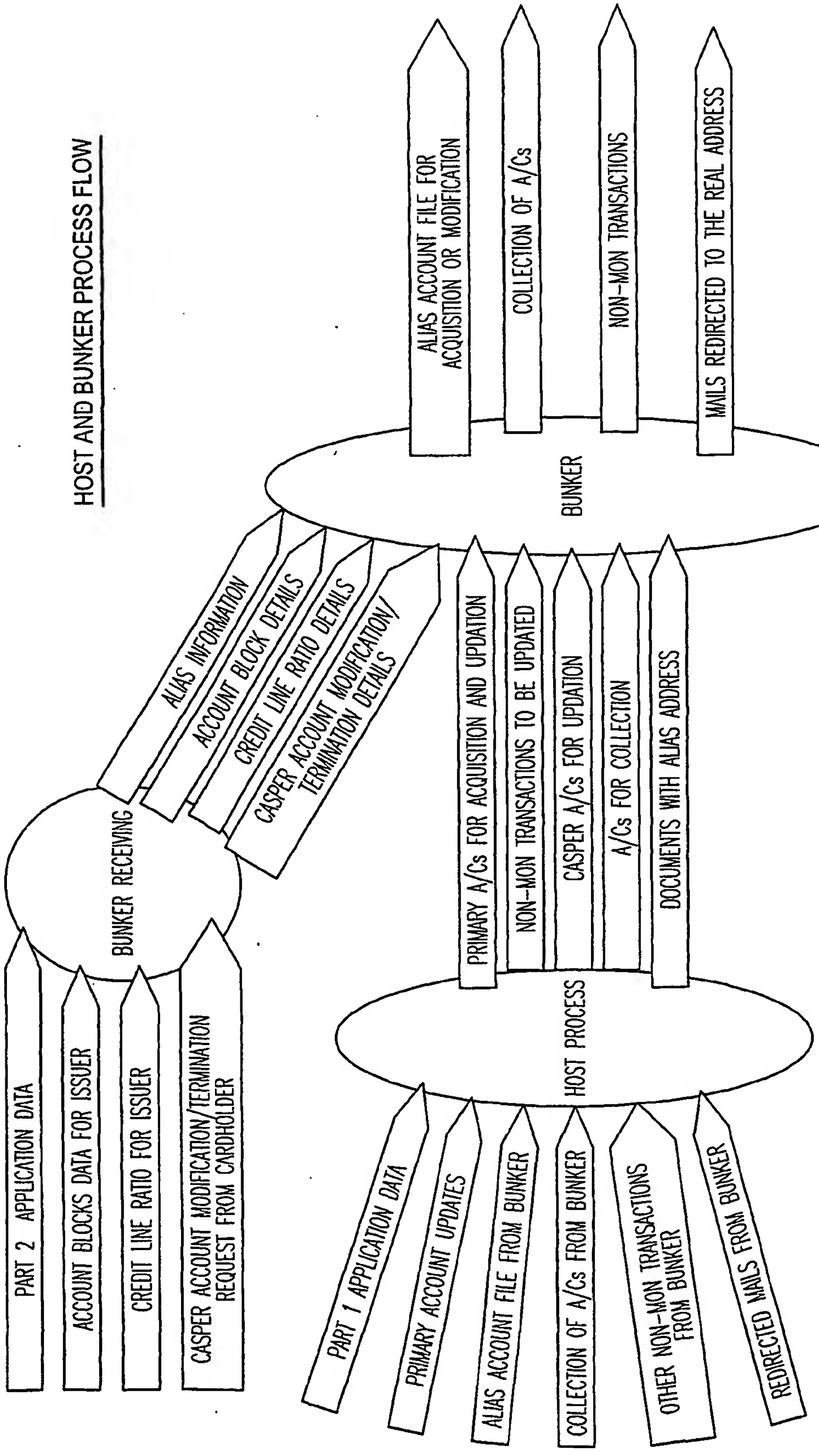

HOST AND BUNKER PROCESS FLOW
BUNKER
ALIAS ACCOUNT FILE FOR ACQUISITION OR MODIFICATION
COLLECTION OF A/Cs
NON-MON TRANSACTIONS
MAILS REDIRECTED TO THE REAL ADDRESS
ALIAS INFORMATION
ACCOUNT BLOCK DETAILS
CREDIT LINE RATIO DETAILS
CASPER ACCOUNT MODIFICATION/ TERMINATION DETAILS
PRIMARY A/Cs FOR ACQUISITION AND UPDATION
NON-MON TRANSACTIONS TO BE UPDATED
CASPER A/Cs FOR UPDATION
A/Cs FOR COLLECTION
DOCUMENTS WITH ALIAS ADDRESS
BUNKER RECEIVING
PART 2 APPLICATION DATA
ACCOUNT BLOCKS DATA FOR ISSUER
CREDIT LINE RATIO FOR ISSUER
CASPER ACCOUNT MODIFICATION/TERMINATION REQUEST FROM CARDHOLDER
HOST PROCESS
PART 1 APPLICATION DATA
PRIMARY ACCOUNT UPDATES
ALIAS ACCOUNT FILE FROM BUNKER
COLLECTION OF A/Cs FROM BUNKER
OTHER NON-MON TRANSACTIONS FROM BUNKER
REDIRECTED MAILS FROM BUNKER

FIG. 12

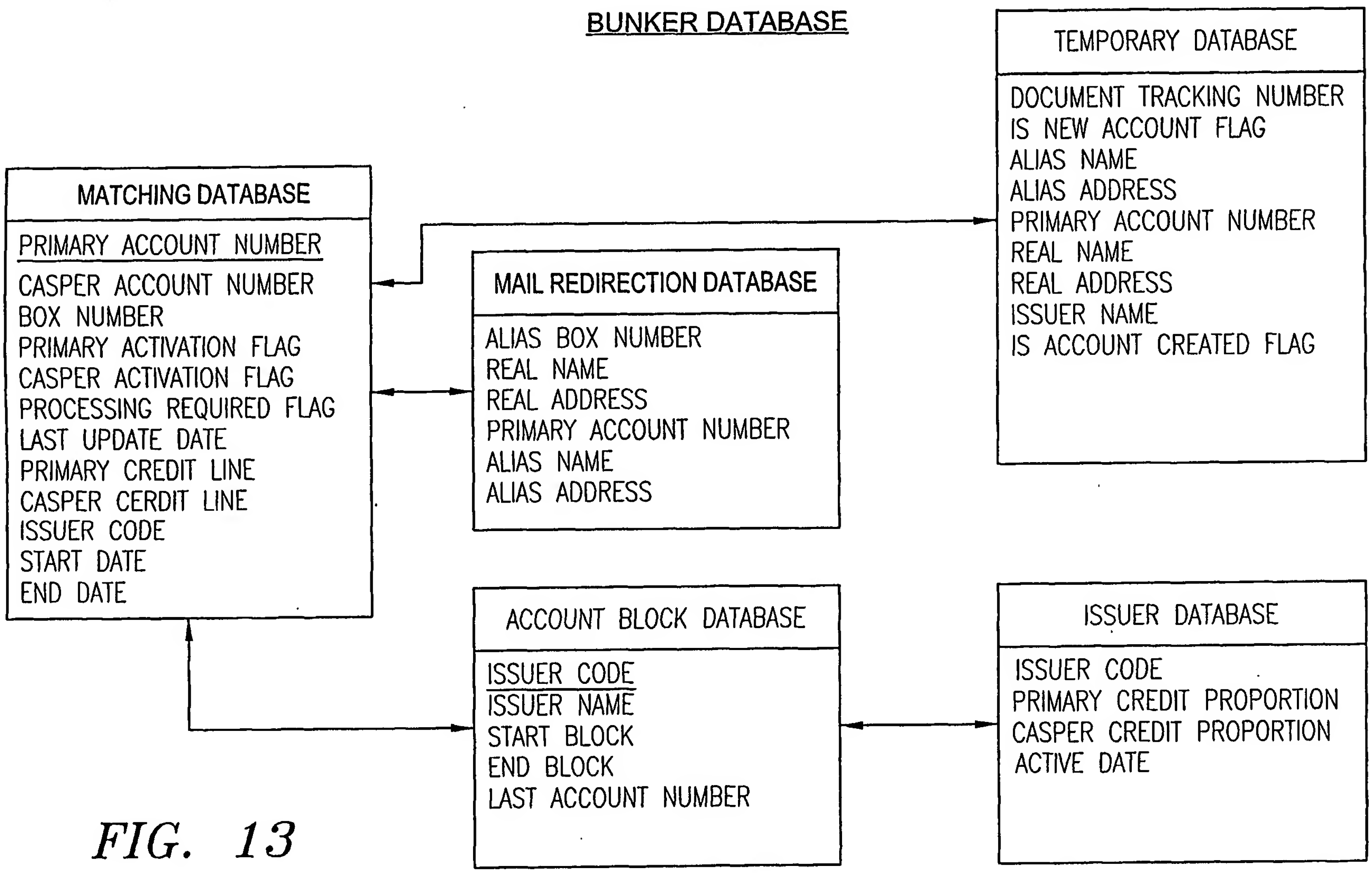

BUNKER DATABASE
MATCHING DATABASE
PRIMARY ACCOUNT NUMBER
CASPER ACCOUNT NUMBER
BOX NUMBER
PRIMARY ACTIVATION FLAG
CASPER ACTIVATION FLAG
PROCESSING REQUIRED FLAG
LAST UPDATE DATE
PRIMARY CREDIT LINE
CASPER CERDIT LINE
ISSUER CODE
START DATE
END DATE
MAIL REDIRECTION DATABASE
ALIAS BOX NUMBER
REAL NAME
REAL ADDRESS
PRIMARY ACCOUNT NUMBER
ALIAS NAME
ALIAS ADDRESS
TEMPORARY DATABASE
DOCUMENT TRACKING NUMBER
IS NEW ACCOUNT FLAG
ALIAS NAME
ALIAS ADDRESS
PRIMARY ACCOUNT NUMBER
REAL NAME
REAL ADDRESS
ISSUER NAME
IS ACCOUNT CREATED FLAG
ACCOUNT BLOCK DATABASE
ISSUER CODE
ISSUER NAME
START BLOCK
END BLOCK
LAST ACCOUNT NUMBER
ISSUER DATABASE
ISSUER CODE
PRIMARY CREDIT PROPORTION
CASPER CREDIT PROPORTION
ACTIVE DATE

FIG. 13

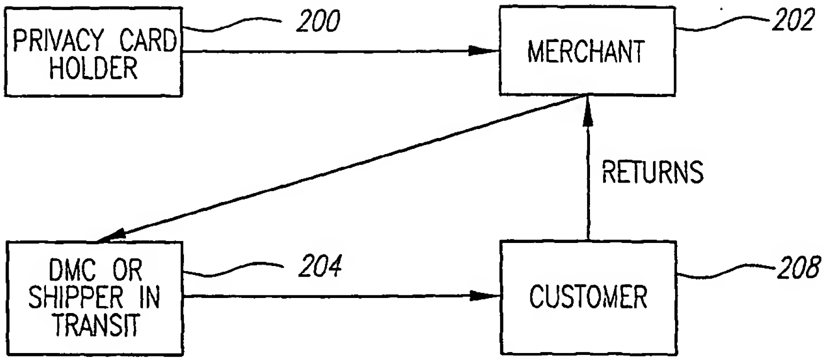

PRIVACY CARD HOLDER
200
MERCHANT
202
RETURNS
DMC OR SHIPPER IN TRANSIT
204
CUSTOMER
208

FIG. 14

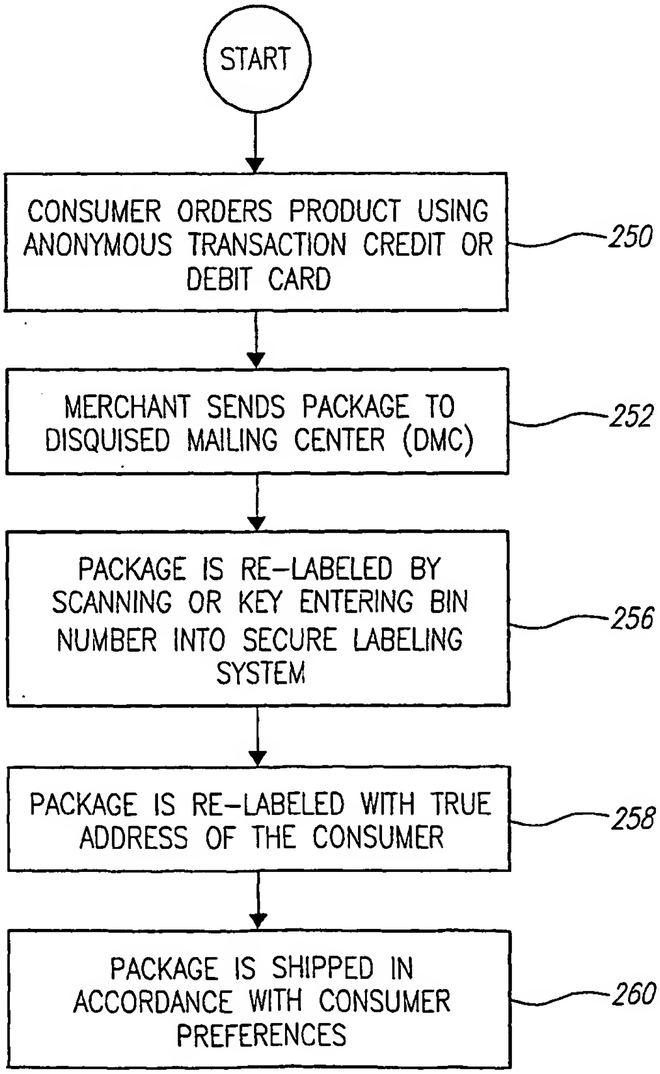

START
CONSUMER ORDERS PRODUCT USING ANONYMOUS TRANSACTION CREDIT OR DEBIT CARD
250
MERCHANT SENDS PACKAGE TO DISQUISED MAILING CENTER (DMC)
252
PACKAGE IS RE-LABELED BY SCANNING OR KEY ENTERING BIN NUMBER INTO SECURE LABELING SYSTEM
256
PACKAGE IS RE-LABELED WITH TRUE ADDRESS OF THE CONSUMER
258
PACKAGE IS SHIPPED IN ACCORDANCE WITH CONSUMER PREFERENCES
260

FIG. 15

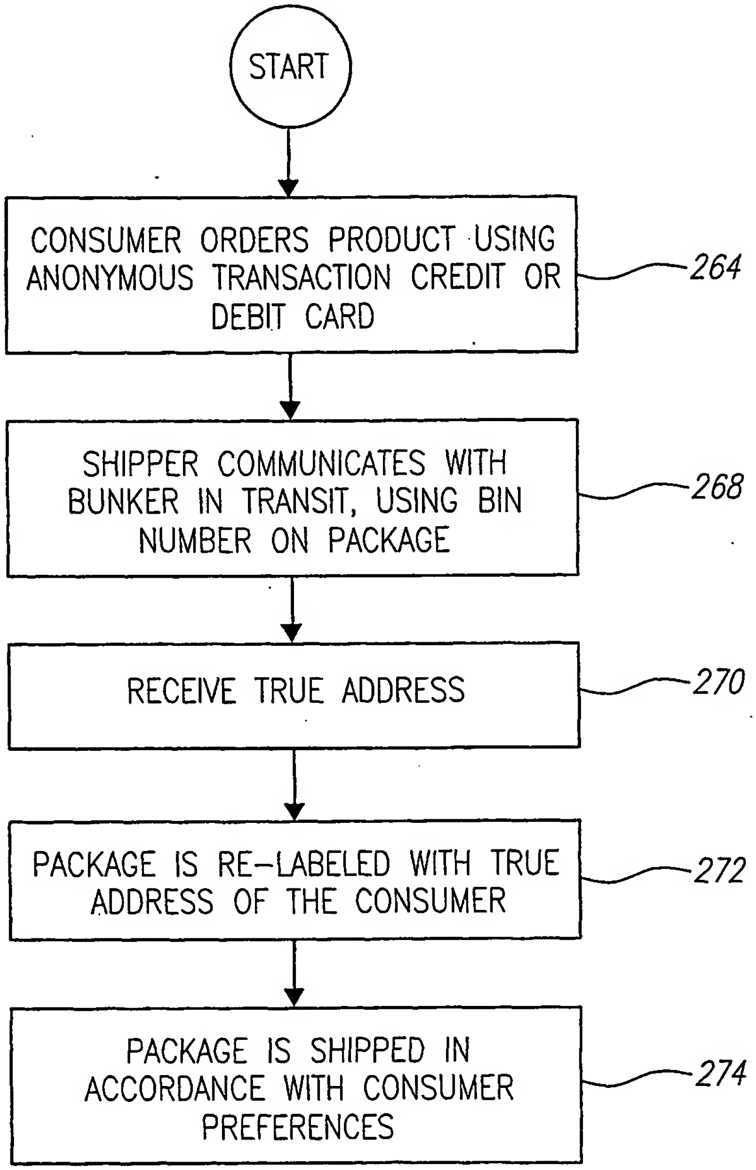

START
CONSUMER ORDERS PRODUCT USING ANONYMOUS TRANSACTION CREDIT OR DEBIT CARD
264
SHIPPER COMMUNICATES WITH BUNKER IN TRANSIT, USING BIN NUMBER ON PACKAGE
268
RECEIVE TRUE ADDRESS
270
PACKAGE IS RE-LABELED WITH TRUE ADDRESS OF THE CONSUMER
272
PACKAGE IS SHIPPED IN ACCORDANCE WITH CONSUMER PREFERENCES
274

FIG. 16

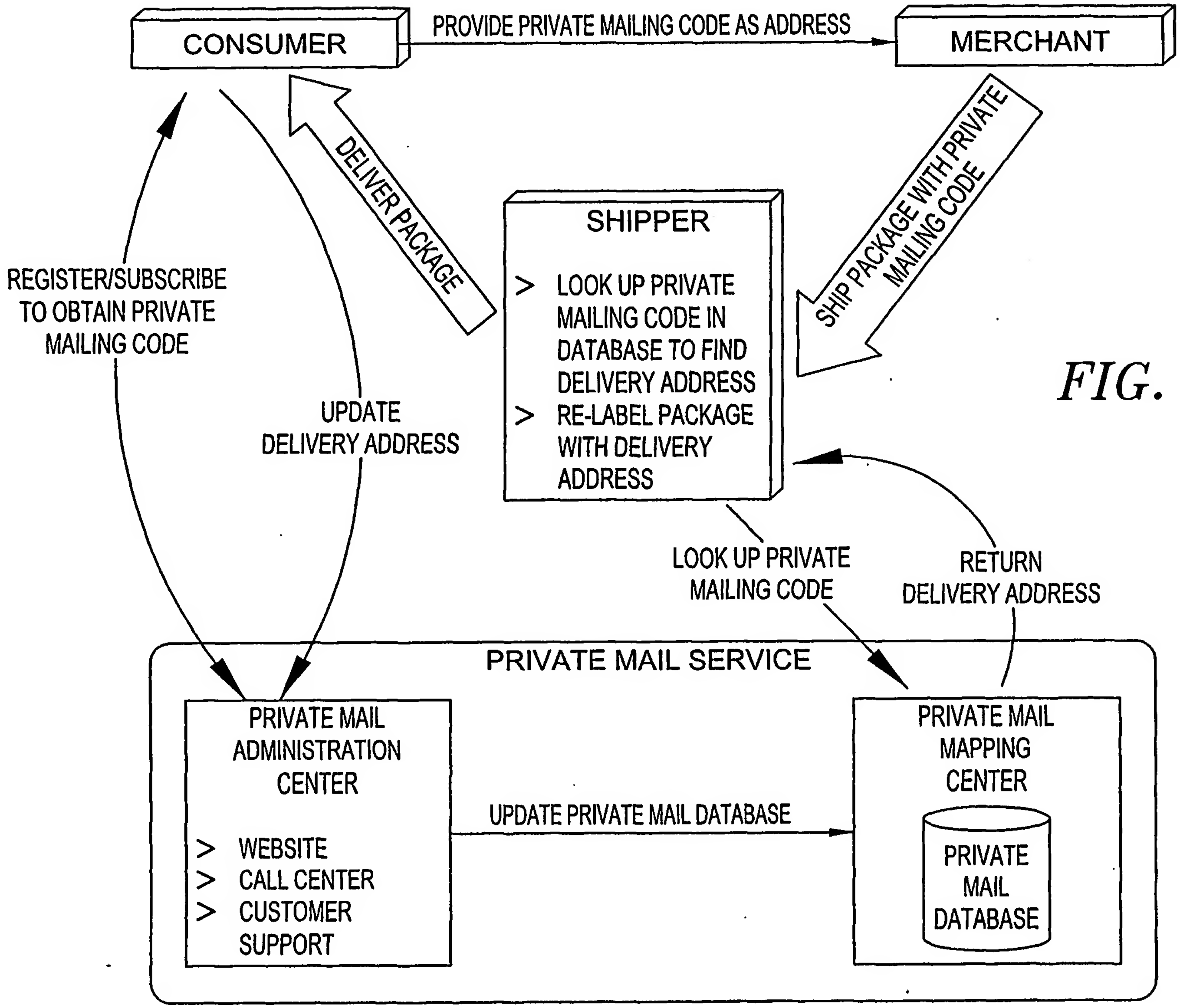

CONSUMER
PROVIDE PRIVATE MAILING CODE AS ADDRESS
MERCHANT
SHIP PACKAGE WITH PRIVATE MAILING CODE
DELIVER PACKAGE
SHIPPER
> LOOK UP PRIVATE MAILING CODE IN DATABASE TO FIND DELIVERY ADDRESS
> RE-LABEL PACKAGE WITH DELIVERY ADDRESS
REGISTER/SUBSCRIBE TO OBTAIN PRIVATE MAILING CODE
UPDATE DELIVERY ADDRESS
LOOK UP PRIVATE MAILING CODE
RETURN DELIVERY ADDRESS
PRIVATE MAIL SERVICE
PRIVATE MAIL ADMINISTRATION CENTER
> WEBSITE
> CALL CENTER
> CUSTOMER SUPPORT
UPDATE PRIVATE MAIL DATABASE
PRIVATE MAIL MAPPING CENTER
PRIVATE MAIL DATABASE

FIG. 17

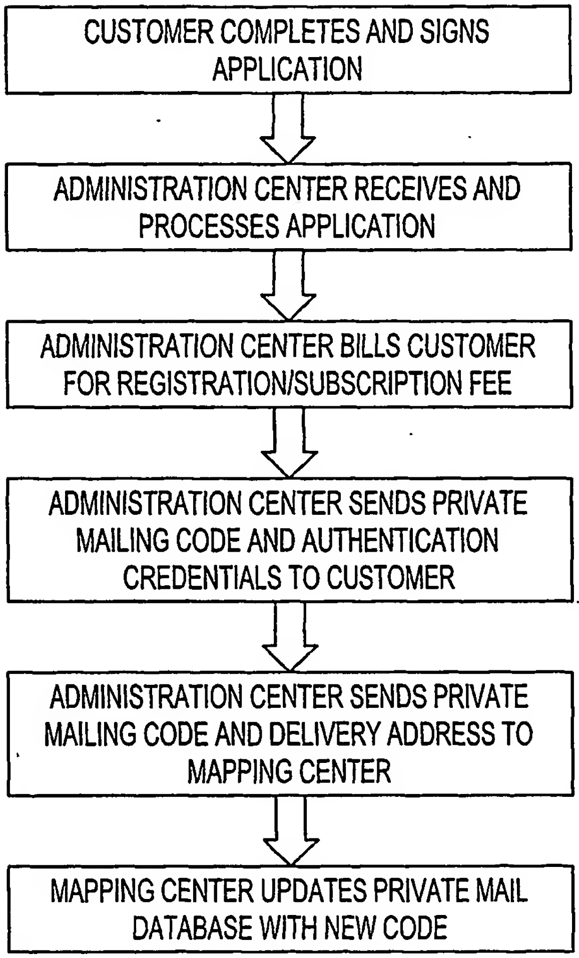

CUSTOMER COMPLETES AND SIGNS APPLICATION
ADMINISTRATION CENTER RECEIVES AND PROCESSES APPLICATION
ADMINISTRATION CENTER BILLS CUSTOMER FOR REGISTRATION/SUBSCRIPTION FEE
ADMINISTRATION CENTER SENDS PRIVATE MAILING CODE AND AUTHENTICATION CREDENTIALS TO CUSTOMER
ADMINISTRATION CENTER SENDS PRIVATE MAILING CODE AND DELIVERY ADDRESS TO MAPPING CENTER
MAPPING CENTER UPDATES PRIVATE MAIL DATABASE WITH NEW CODE

FIG. 18

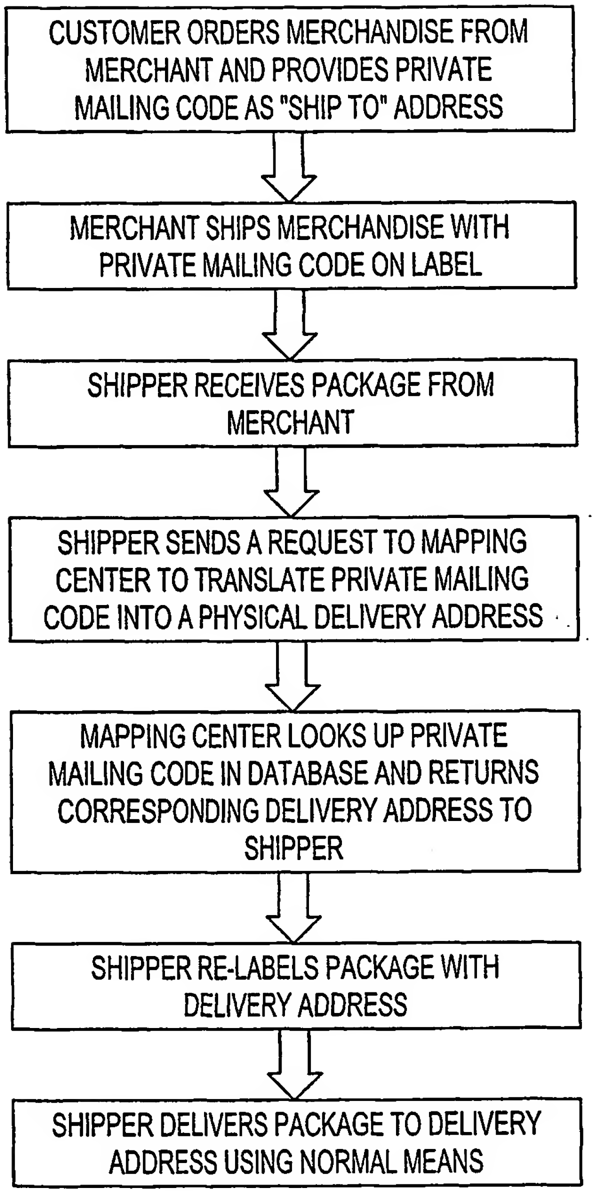

CUSTOMER ORDERS MERCHANDISE FROM MERCHANT AND PROVIDES PRIVATE MAILING CODE AS "SHIP TO" ADDRESS
MERCHANT SHIPS MERCHANDISE WITH PRIVATE MAILING CODE ON LABEL
SHIPPER RECEIVES PACKAGE FROM MERCHANT
SHIPPER SENDS A REQUEST TO MAPPING CENTER TO TRANSLATE PRIVATE MAILING CODE INTO A PHYSICAL DELIVERY ADDRESS
MAPPING CENTER LOOKS UP PRIVATE MAILING CODE IN DATABASE AND RETURNS CORRESPONDING DELIVERY ADDRESS TO SHIPPER
SHIPPER RE-LABELS PACKAGE WITH DELIVERY ADDRESS
SHIPPER DELIVERS PACKAGE TO DELIVERY ADDRESS USING NORMAL MEANS

FIG. 19